Maksuvälinepetos ja sen kehittyvät tekotavat

Niko Tonteri

5/2024

Poliisiammattikorkeakoulun opinnäytetyö / AMK

TIIVISTELMÄ

Tekijät: Niko Tonteri: Maksuvälinepetos ja sen kehittyvät tekotavat
Opinnäytetyön muoto: Oikeusdogmaattinen, kirjallisuuskatsaus
Julkisuusaste: Julkinen
Ohjaajat: Päivi Salminen ja Lauri Tammiaho
Tutkinto: Poliisi (AMK)

Opinnäytetyössä käsitellään rikoslain 37 luvun 8§:n mukaista maksuvälinepetosta. Sen tarkoituksena on esitellä maksuvälinepetosta rikoksena. Tämän lisäksi käsitellään maksuvälinepetoksien tekotapoja ja maksuvälinettä – ja etenkin maksuvälineen kehittymistä – suhteellisen uudessa rikoslajissa. Opinnäytetyön tutkimusmenetelminä käytetään oikeusdogmaattista lähestymistapaa, sekä kirjallisuuskatsausta. Maksuvälinepetosten määrä on kasvava, huolimatta niin viranomaisten kuin rahoituslaitoksien ohjeista ja varoituksista huolimatta.

Yleisesti tiedämme, että tietoliikenne internetissä on kasvanut räjähdysmäisesti 2000-luvulla teknologian kehittymisen myötä. Teknologisen kehittymisen lisäksi verkossa tapahtuva asiointi, osto- ja myyntitapahtumat, sekä henkilökohtainen viestintä on tullut saavutettavaksi, helpommaksi ja arkiseksi kanssakäymiseksi, ja ihmisten tietoisuus kehittyy jatkuvasti virtuaalisesta maailmasta. Tietoisuus internetin tarjoamista hyödyistä on sulautunut lähes jokaisen meidän päivittäiseen elämäämme. Kaupankäyntivälineet ja -menetelmät ovat mahdollistaneet, myös maksuvälinepetoksia tekeville uusia tapoja ja menetelmiä.

Opinnäytetyöni tarjoaa tietoa internetin varjopuolista, mitä voi tarkastella maksuvälinepetosten näkökulmasta. Opinnäytetyö avasi maksuvälinepetoksen tunnusmerkistön rikosoikeudellisen sisällön lisäksi yhden kaikkia viranomaisia haastavan rikoslajin. Poliisin osalta epäiltyjen rikoksien tutkimista voi haastaa se, että rikoksia tehdään ympäri maailmaa ja rikoksen tekijä voi tehdä useitakin rikoksia lyhyessä aikaa. Kuitenkin maksuvälinepetos – kuten muutkin petokset – olisi lähtökohtaisesti selvitettävissä lähes aina. Itselleni opinnäytetyön perusteella jäi yhdeksi keskeiseksi näkökulmaksi ja ajatukseksi, että ennalta ehkäisy – oli se sitten varmennepalvelun tai viranomaisten ansiota – on tehokkaampi tapa torjua maksuvälinepetoksia. Ainakin asianomistajan näkökulmasta, sillä vaikka rikos saataisiinkin selvitettyä jää rikoksella aiheutettu vahinko harmittavan usein saamatta takaisin.

Sivumäärä: 35

Tarkastuskuukausi ja vuosi: Toukokuu 2024

Avainsanat: Maksuvälinepetos, maksuväline ja tekotapa

ABSTRACT

Authors: Niko Tonteri: Payment card fraud and its evolving methods.
Type of thesis: *Research-based thesis, practice-based thesis*
Publicity: Public
Supervisors: Päivi Salminen and Lauri Tammiaho
Degree: Bachelor of police services

The thesis addresses payment card fraud according to Section 8 of Chapter 37 of the Penal Code. Its purpose is to present payment card fraud as a criminal offense. In addition, it discusses the methods of payment card fraud and the payment instrument – especially the evolution of payment cards – in a relatively new criminal law context. The research methods employed in the thesis include a legal-dogmatic approach and a literature review. The number of payment card frauds is increasing, despite guidance and warnings from authorities and financial institutions.

It is widely known that internet communication has grown explosively in the 21st century with the advancement of technology. In addition to technological advancements, online transactions, buying and selling, as well as personal communication, have become more accessible, easier, and commonplace, and people's awareness of the virtual world continues to evolve. Awareness of the benefits offered by the internet has become integrated into almost every aspect of our daily lives. Trading tools and methods have also enabled new ways and techniques for those committing payment card fraud.

My thesis provides insights into the darker aspects of the internet, focusing on the perspective of payment card fraud. In addition to delving into the legal elements of payment card fraud, the thesis explores one of the most challenging types of crime for all authorities. From the perspective of law enforcement, investigating suspected crimes can be challenging, especially considering that these crimes occur globally, and perpetrators can commit multiple offenses in a short period. However, payment card fraud, like other forms of fraud, is typically solvable in almost all cases. Through my thesis, one key perspective and insight that emerged for me is the importance of prevention—whether through authentication services or law enforcement—in effectively combating payment card fraud. From the standpoint of the victim, even if the crime is resolved, the damage caused by the crime often remains uncompensated.

Pages: 35

Month and year of review: May 2024

Keywords: Payment card fraud, payment instrument and methods

SISÄLLYS

1 JOHDANTO

1.1 Johdatus aiheeseen

Opinnäytetyössäni tutkin maksuvälinepetoksien tekotapoja ja maksuvälinepetosta rikoksena. Idea tästä aiheesta syntyi, kun luin artikkelin, jossa vanhempi herra oli joutunut huijatuksi hotellivarausta tehdessä. Vanhempi herra oli maksanut tekaistulle internet-sivulle varauksesta, jota koskaan ei tapahtunut, ja samalla hän menetti varauksessa käyttämänsä luottokorttitiedot. Rikostyyppi ja sen moninaiset tekotavat ovat lisääntyneet internetin mahdollistaman eri maksualustojen moninaisuuden ja erityisesti kasvaneen verkko-ostoskäyttäytymisen takia. Toistaiseksi ei maksuvälinepetoksien kasvua ole saatu vähenemään, vaan päinvastoin se haastaa poliisiin rikostutkintaa yhä enemmän.

Hain tietoa maksuvälinepetoksista ja niiden kehittymisestä. Tietoa hakiessani huomasin nopeasti, että maksuvälinepetoksien määrässä on havaittavissa selkeä piikki vuonna 2023. Totesin, että tästä oli saatavilla vain vähän dataa ja aineistoa, joten päätin keskittyä tutkimaan maksuvälinepetosta rikoksena ja sen erilaisia tekotapoja. Maksuvälinepetos ja sen kehittyvät tekotavat on ajankohtainen, sillä teknologian hurja kehitys on ajanut rikollisuutta uusille pelikentille, sekä avannut ovia tekotavoille, joista viime vuosisadalla ollut puhettakaan. Edelliseltä vuosikymmeneltäkin on edetty entistä kehittyneempiin maksuvälinepetoksen tekotapoihin.

Internetin ja viestinnän kehittyminen on antanut maksuvälinepetoksille uusia tuulia. Netin käytön räjähdysmäinen lisääntyminen ja sen arkipäiväinen käyttö tarjoaa rikollisille uuden pelikentän. Maksuvälinepetos voidaan siis tänä päivänä tehdä toisellakin tapaa, kuin käyttämällä luvatta kaverin pankkikorttia. Tekotapoja on lukuisia ja tässä työssä on tuotu yhteen tapoja, jotka ovat tunnettuja ja niistä löytyy jo ennalta tietoa. Työn tarkoituksena on osoittaa ja kertoa maksuvälinepetoksesta ja sen luonteesta, sekä tuoda esille sen nykypäiväisiä tekotapoja. kuinka paljon maksuvälinepetosten määrä on muuttunut neljän vuoden aikana.

Aihe antaa myös lukijalle näkökulmaa ja ajatuksia maksuvälinepetosten tekotapojen myötä internet tietoisuudelle, vaikka työssä ei erityisesti syitä maksuvälinepetoksien kasvulle käydäkään läpi. Työ on toteutettu kokonaan julkisia lähteitä käyttäen, joten se on julkisesti luettavissa. Opinnäytetyö voi hyödyntää kaikenikäiset ihmiset, eikä työtä ole suunnattu tietylle ryhmälle, mutta erityisesti työ antaa itselleni näkökulman tämän päivän hyvin yleiselle ja yleistyvälle rikoslajille, jonka kaikkia tekotapoja emme vielä ole nähneet.

Maksuvälinepetos on rikoslajina uusi ja voimakkaasti kasvava, joka vaatii viranomaisilta paljon resursseja ja osaamista ja kiinnittää erityisesti huomiota ennalta ehkäisyyn. Maksuvälinepetos on tyypillisesti sellainen, että yksi henkilö tekee useita rikoksia. Lähtökohtaisesti maksuvälinepetokset olisivat selvitettävissä ja ennalta estettävissä, mikäli asianosainen henkilö olisi riittävän huolellinen ja internettiä käytettäisiin turvallisesti, erityisesti maksutapahtumien yhteydessä.

1.2 Tutkimuskysymykset ja aiheen rajaaminen

Opinnäytetyöni tarkastelee rikoslain 37 luvun mukaista maksuvälinepetosta ja sen yleisiä tekotapoja. Työssäni käsitellään maksuvälinettä ja nykypäivän yleisimpiä maksuvälineitä ja maksutapoja. Vuonna 2022 yleisimmin käytettiin päivittäistavaraostoksissa Debit-korttia 73 %, luotollista creditkorttia 11 %, käteistä 6 % ja kaupparyhmän maksu- tai luottokorttia 4 %. Maksamiseen tarkoitetuista sovelluksista suosituin oli Apple Pay 5 %, muiden sovelluksien käyttö oli 1 %:n luokkaa (Finanssiala 2023). Mobiilimaksamisen suosio on kasvanut ja erilaisia mobiililompakoita ja sovelluksia on tarjolla, mutta ainakin vielä tänä päivänä valtaväestö suosii viime vuosisadan puolella Suomeen rantautunutta maksukorttia (Yle 2010).

Opinnäytetyössäni olen rajannut tavoitteekseni keskittyä maksuvälinepetokseen ja sen perusmuotoon. Rajaan ulkopuolelle rikosnimikkeet, jotka sinällään voivat olla oheisrikoksena, tai edellytyksenä tarkastelemalleni rikoslajille – maksuvälinepetos – esimerkiksi: identiteettivarkaus (RL 38:9 a §), väärän henkilötiedon antamisesta viranomaiselle (RL 16:5 §), viestintäsalaisuudenloukkaus (RL 38:3 §), tietomurto (RL 38:8 §), maksuvälinerikos (RL 37:12 §), sekä varkaus (RL 28:1 §) ja petos (RL 36:1 §).

Rajaan myös asianomistajan profiloinnin - siis onko vaikka vanhemmat ihmiset, ja ne, joilla ei välttämättä ole kokemusta tai osaamista turvallisesta ja vastuullisesta verkossa toimimisesta. Lisäksi on olemassa bulvaanin käyttöä, jossa käytetään hyväksi kolmatta, ehkä hyväuskoista, pakotettua tai lahjottua henkilöä toteuttamaan rikos. Asianomistajan oma mahdollinen huolimattomuus tai erehtyminen, joka sinällään on oleellista suurenkin vahingon toteutumiseksi, ovat tämän työn ulkopuolella, sillä ne voisivat toimia omana työnään jo pelkästään niiden laajuuden vuoksi.

Opinnäytetyön alkaa johdannolla, jossa lukija johdatetaan aihepiiriin, jonka jälkeen avataan maksuvälineen käsitettä, jotta opinnäyte on kokonaisuudessaan helppo lukuinen. Opinnäytetyön seuraava osa käsittelee maksuvälinepetoksen lakiperustaa ja maksuvälinepetosta käydään läpi sopivassa laajuudessa työn tarkoitukseen nähden. Rikoslain 37 luku pitää sisällään maksuvälinerikoksia ja tässä tutkimuksen ensimmäisessä osassa perehdytään maksuvälinepetoksiin eli rikoslain 37 luvun 8–11 §:iin. Edellä mainitut pykälät sisältävät lievän, perusmuotoisen ja törkeän maksuvälinepetoksen, sekä maksuvälinepetoksen valmistelun. Muita rikoslain 37 luvun maksuvälinerikoksia tässä tutkimuksessa ei käsitellä.

Kolmannessa kappaleessa käsitellään nykypäivän maksuvälineitä, jotka määritellään rikoslain 37 luvun 15 §:n 1 momentin 2 kohdassa. Tänä päivänä maksutapoja on lukuisia ja näistä käytetyimpiin otetaan kantaa opinnäytetyössäni, jotka tukevat tutkimuksen kokonaisuutta. Viimeinen osa ennen tutkimuksen johtopäätöksiä käsittelee maksuvälinepetoksen tunnettuja tekotapoja. Kaikkia mahdollisia maksuvälinepetosten tekotapoja ei opinnäytetyön laajuuden vuoksi tosin käydä läpi ja kehitys tekotapojen osalta on nopeaa, joten on mahdollista, että viranomaisillakaan ei ole aivan uusimmista tekotavoista tarkkaa tietoa.

Tutkimuskysymykseni rakentuvat kolmen kysymyksen ympärille, jotka samalla ovat myös osa tämän opinnäytteen läpileikkaavia teemoja. Tutkimuskysymykset, ja niiden ympärille rakentuva oikeusdogmaattiseen ja kirjalliskatsaukseen perustuva opinnäyte eivät ole absoluuttisen täydellinen kyseistä rikoslajia avaava teos, vaan kuten johtopäätöksissäni totean vain enemmän maksuvälinepetoksen perusnormin kuvaava tutkimus, joka jättää niin rikosoikeudelliselle tulkinnalle kuin tekotavoille liikkumatilaa. Alla olevien kolmen kysymyksen mukaisesti tutkimus käsittelee ja kuvaa rikoslajin laajuutta.

Tutkimuskysymykset:

-Mikä on maksuvälinepetos?

-Mikä on maksuväline?

-Miten maksuvälinepetoksia tehdään?

1.3 Tietoperusta ja tutkimusmenetelmä

Opinnäytetyö työ toteutetaan oikeusdogmaattisena tutkimuksena ja kirjallisuuskatsauksena. Maksuvälinepetoksen lainopillinen tarkastelu ja oikeussäännöstentulkinta on opinnäytetyöni lainopillista tutkimusta. Maksuvälineestä ja maksuvälinepetosten tekotapoja tutkiva osuus on opinnäytetyön kirjallisuuskatsausta hyödyntävää tutkimusmenetelmää. Opinnäytetyön tarkoituksena on osoittaa maksuvälinepetosten kehitystä tekotapojen, määrän ja lakien pohjalta. Aineisto opinnäytetyölleni koostuu rikoslaista, tilastoista, artikkeleista ja kirjallisuudesta. Nämä edellä mainitut aineistot on hankittu julkisesta verkosta avoimia lähteitä käyttäen ja tarvittavan kirjallisuuden kirjastosta. Aineistosta on tarkoitus kerätä tietoa, jota voidaan analysoida ja luoda mahdollisimman tarkka kuvaus tutkittavasta aiheesta.

Opinnäytetyössäni hyödynnetään oikeusdogmaattista metodia, joka keskittyy lainopillisen tiedon tutkimiseen. Oikeusdogmatiikka käsittelee positiivista eli säädettyä oikeutta. Tässä tutkimusmenetelmässä tulkitaan ja arvioidaan oikeudellisia tekstejä sekä järjestelmällisesti järjestetään niitä (Aarnio 1989, 47–48). Lainopin päätehtäviin kuuluvat oikeuden tulkinta ja systematisointi, jotka ovat

keskinäisesti riippuvaisia. Oikeuden tulkinnassa pyritään ymmärtämään positiivisen oikeuden normien merkitystä ja sisältöä. (Tuori 2007, 27.)

Kirjallisuuskatsaus on tieteellinen tutkimusmenetelmä, jossa kootaan ja arvioidaan olemassa olevaa tietoa tietyltä aihealueelta, tarkoituksenaan vastata tutkimuskysymykseen tai -ongelmaan. Sen avulla tutkija esittelee lukijakunnalle aiheesta tehdyt aikaisemmat julkaisut ja tutkimukset, tiivistäen ja analysoimalla niiden keskeiset havainnot ja tulokset. Kirjallisuuskatsauksia on erilaisia ja niiden laatu ja laajuus vaihtelevat riippuen tutkimusaiheesta ja tavoitteista. Yleisesti ottaen kirjallisuuskatsauksen avulla muodostuu kokonaiskuva olemassa olevasta tutkimustiedosta ja sen merkityksestä kyseisellä tutkimusalueella. Kirjallisuuskatsauksen vaiheet voidaan karkeasti jakaa kolmeen osaan. Ensimmäinen vaihe sisältää katsauksen suunnittelun, toinen vaihe käsittää katsauksen tekemisen hakuineen ja kolmas vaihe sisältää analyysin ja johtopäätökset. Suunnitteluvaiheessa määritellään tutkimuskysymykset, joiden pohjalta katsaus rakennetaan. (Johansson, Axelin, Stolt, Ääri, 2007, 3-5.)

Opinnäytetyön näkökulma ja tarkoitus huomioon ottaen lähdeaineistosta keskeinen osa koostuu lainvalmistelu aineistosta, kuten hallituksen esityksistä. Käytän opinnäytetyössä rikoslakia ja etenkin 37 lukua, josta löytyy säädös maksuvälinepetoksista. Kirjallisuuslähteet luovat, myös suuren osan opinnäytetyön kokonaisuudesta. Tekotapoja tutkivassa osassa on käytetty laajasti lähteenä Europolin ja Enisan vuosiraportteja, jotka antavat ajankohtaista tietoa kyberrikollisuudesta, josta löytyy paljon aineistoa maksuvälinepetoksista ja rikollisuuden muodoista, jotka tuottavat maksuvälinepetoksia sivutuotoksena. Kokonaisuudessaan tutkimukseen valitut lähteet tukevat tutkimuksen luotettavuutta ja tavoitetta. Lisäksi kuviot, jotka sisältävät tilastotietoa tutkittavasta aiheesta auttavat hahmottamaan maksuvälinepetosten nykytilannetta ja niiden kehitystä Suomessa ja tukevat opinnäytetyöni kokonaisuutta.

Maksuvälinepetoksista kertovaa kirjallisuutta löytyy kirjastosta, joita hyödynnän opinnäytetyössäni lähteenä ja tukipilareina tutkimukselle. Kirjallisuudesta löytyvää tietoa vertailen, myös muuhun tietoon, jota olen kerännyt organisaatioiden internet-sivuilta ja artikkeleista. Vanhempi kirjallisuus tarjoaa myös maksuvälinepetosten tekotavan tarkastelun ja sen tulkinnan muutoksen pidemmällä ajanjaksolla. Tulkinta ja soveltamiskäytäntö liittyvät rikoslajin laajenemiseen mm. yrityksen muodossa, mutta erityisesti rikoksen toteutumisen eri muotoina.

2 YLEISTÄ

Rikoslain kokonaisuudistuksen ensimmäisen vaiheen myötä 37 luku maksuvälinerikoksista tuli voimaan vuoden 1991 alusta. Luvun 8 §:n säännös maksuvälinepetoksesta edusti uudenlaista rikostyyppiä. Sen tavoitteena oli muun muassa ratkaista aiemmin esiintyneitä rajanveto-ongelmia oikeuskäytännössä. (HE 38/1997.)

1990-luvun lopun tietotekniikan kehitys on mahdollistanut uudenlaisia muotoja rahaliikenteelle. Esimerkiksi shekit ovat lähes kokonaan poistuneet käytöstä, ja käteisen rahan merkitys maksuvälineenä on vähentynyt merkittävästi. Perinteiset kortit, joissa informaatio tallennettiin magneettijuovalle tai kohokirjoituksena, korvataan nyt sirukorteilla. (HE 38/1997.)

Maksuvälineissä ja sen määritelmässä on tapahtunut hurjaa muutosta ja arkipäiväisiä asioita hoidetaan tänä päivänä täysin eri tavalla, kun vielä ennen vuosituhannen vaihdetta, kuten vuoden 1997 voimaan tulleessa hallituksen esityksessä mainitaan. Maksuvälineiden uudenlainen merkitys ja maksuvälinepetos on siis rikoksena varsin uusi ja sen kehitys on ainakin tähän päivään asti ollut merkittävää ja syytä kehityksen loppumiselle ei ole tiedossa. Uudenlaiset maksutavat ja maksupalvelut tuovat rikollisuudelle uusia mahdollisuuksia.

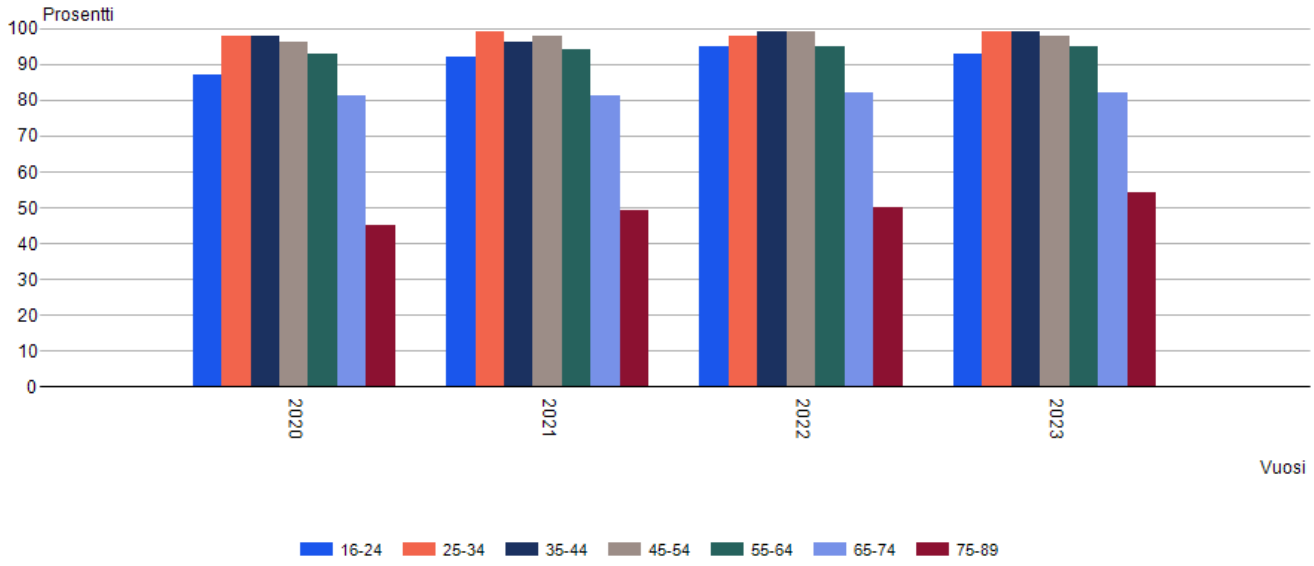
2.1 Internetin käytön lisääntyminen

Teknologia on keskeinen osa modernin yhteiskunnan toimintaa ja kehitystä. Sen vaikutus ulottuu lähes kaikille elämänaloille, mukaan lukien talous, terveys, viestintä, koulutus ja viihde. Teknologinen innovaatio ja kehitys ovat olennainen tekijä taloudellisessa kasvussa. Uudet teknologiat ja digitaaliset ratkaisut luovat uusia työpaikkoja, tehostavat tuotantoa ja parantavat yritysten kilpailukykyä kansainvälisillä markkinoilla. Teknologia mahdollistaa välittömän tiedonvälityksen ja viestinnän yli maantieteellisten esteiden. Internet, älypuhelimet ja sosiaalinen media tarjoavat kanavia tiedon jakamiseen ja vuorovaikutukseen miljardeille ihmisille ympäri maailmaa. (Thomas ym. 2022, 3.)

Teknologiset innovaatiot parantavat yhteiskunnan turvallisuutta ja valvontaa. Esimerkiksi valvontakamerat, biometriset tunnistusjärjestelmät ja tekoälypohjaiset turvallisuussovellukset auttavat ehkäisemään rikollisuutta ja suojelemaan kansalaisia. Modernissa yhteiskunnassa teknologian merkitys on valtava ja monitahoinen. Sen vaikutukset ulottuvat lähes kaikille elämänalueille ja sen jatkuva kehitys muokkaa yhteiskuntaa ja ihmisten tapaa toimia, kommunikoida ja ajatella. (Thomas ym. 2022, 3.)

Valtaväestö lähes kaikissa ikäluokissa käyttää internetiä apunaan arkipäiväisissä asioissa. Internet helpottaa ja nopeuttaa arjen perusasioiden hoitamista. Alla olevaa kuviota tarkastelemalla voidaan

havaita, että kaikki 16–74-vuotiaat henkilöt ovat käyttäneet internetiä ja nykyaikaisia viestintävälineitä apunaan hoitaessa pankkiasioita vähintään kolmen kuukauden sisällä viimeisen neljän vuoden ajan. Vanhimmalla ikäluokalla, joka kuviosta 1 käy ilmi ovat 75–89-vuotiaat henkilöt. Vanhimmalla ikäluokalla viestintätekniikoiden apuna käyttäminen vuonna 2020 on ollut noin 45 % ja on ollut jokaisena vuonna kasvussa. Vuonna 2023 internetin avulla 55 % henkilöistä on hoitanut pankkiasioitaan, jotka ovat sijoittuneet 75–89-vuotiaiden ikäryhmään. 25–54 vuotiaista henkilöistä 95 % ovat käyttäneet eri viestintätekniikoita apunaan pankkiasioita hoitaessaan kolmen kuukauden sisällä. (Kuvio 1.)



KUVIO 1. Väestön tieto- ja viestintätekniikan käyttö tilasto. Ikä ja vuosi muuttujina. Yhteensä hoitanut pankkiasioita viimeisen 3 kuukauden aikana, prosentteina (Tilastokeskus 2024).

2.2 Maksuvälineen määritelmä ja maksuvälinelomake

Rikoslain 37 luvun 15 §:n 1 momentin 2 kohdassa määritellään maksuväline, jonka mukaan maksuvälineellä tarkoitetaan aineetonta tai aineellista suojattua välinettä, tietoteknistä ohjelmaa tai tunnistamistietoa tai muuta vastaavaa yksilöivää tietoa taikka niiden yhdistelmää, joka ei ole käteisrahaa eli seteleitä tai metallirahoja, ja jotka yksin tai yhdessä mahdollistavat sen, että haltija tai käyttäjä voi siirtää rahaa tai rahallista arvoa. Rikoslain 37 luvun mukaisella maksuvälineellä tarkoitetaan siis pankki-, maksu-, tai luottokorttia, shekkiä tai muuta välinettä taikka tallennetta (HE 52/2021 vp, 6). Tämän takia käteistä rahaa ei käsitellä tutkimuksessa, vaikka se virallinen maksuväline onkin (Hallamaa 2020).

Maksuvälineet voivat olla joko yleiskäyttöisiä tai kohdennettuja. Yleiskäyttöiset maksuvälineet ovat käyttökelpoisia laajasti erilaisissa tilanteissa, kun taas kohdennetut maksuvälineet on suunnattu erityisesti tiettyihin käyttötarkoituksiin. Esimerkkejä näistä ovat paperiset ja sähköiset arvopaperit, maksukortit, internet- ja mobiilipalvelut sekä erilaiset sovellukset. (HE 52/2021 vp, 6.)

Hallituksen esityksen mukaan maksuvälineeksi luokitellaan pankki-, maksu- tai luottokortti, shekki tai vastaava väline tai tallenne. Tämän avulla voidaan suorit-taa maksuja, tehdä tilinostoja tai tilisiirtoja, ja sen käyttäminen on välttämätöntä mainittujen toimintojen suorittamiseksi. Pykälän 2 momentissa todetaan, että 37 luvun maksuvälineeseen liittyvät säännökset koskevat myös julkisen valvonnan alaisen luottolaitoksen talletuksesta annettua vastakirjaa ja muita saamistodisteita. (HE 52/2021 vp, 6.)

Maksuvälinelomakkeella tarkoitetaan rikoslain 37 luvun 15 §:n mukaan painettua maksuvälineeksi täydennettävää lomaketta, jota ei ole yleisön mahdollista saada vapaasti. Pykälän mukaan maksuvälinelomakkeella tarkoitetaan, myös korttia tai korttiaihiota, joka soveltuu erityisesti maksuvälineen valmistamiseen.

2.3 Maksuvälinepetos

Maksuvälinepetoksen rangaistavuus ei vaadi erehdyttämistä tai erehtymistä, toisin kuin perinteisen petoksen tapauksessa. Lisäksi maksuvälinepetoksessa ei ole välttämätöntä, että teosta seuraa taloudellista vahinkoa. Riittää, että teolla on ollut potentiaali aiheuttaa taloudellista vahinkoa, jotta se voidaan katsoa rangaistavaksi. Maksuvälinepetokselle on ominaista, että tekijä käyttää maksuvälinettä ilman sen laillisen haltijan lupaa tai ylittää lupaan perustuvan oikeutensa. Lisäksi maksuvälinepetokseen voi syyllistyä käyttämällä väärää maksuvälinettä. Maksuvälinepetoksen tunnusmerkistö täyttyy heti, kun maksuvälinettä käytetään. Tässä yhteydessä "käyttäminen" viittaa maksuvälineen esittämiseen vaihdantatoimessa, jossa sitä on tarkoitettu käytettäväksi. On merkityksetöntä, esitetäänkö maksuvälinettä ihmiselle vai automaatille. (Tapani 2013, 530.)

Rikoslain 37 luvun 8 §:n kahdessa ensimmäisessä kohdassa: Henkilö, joka hankkii itselle tai toiselle oikeudetonta taloudellista hyötyä, käyttää maksuvälinettä ilman sen laillisen haltijan lupaa, lupaan perustuvan oikeutensa ylittäen, muuten ilman laillista oikeutta tai käyttää väärää tai väärennettyä maksuvälinettä on tuomittava maksuvälinepetokseen.

Väärän maksuvälineen käytöstä on korkeimman oikeuden ratkaisu, jossa on ollut käsittelyssä seuraavanlainen maksuvälinepetos: A oli ostanut neljän euron kappale hintaan yhteensä 1385 kappaletta vääriä 8,40 euron arvoisia lounasseteleitä, joita oli sitten myynyt eteenpäin 5 euron kappalehintaan, sekä luovuttanut seteleitä eteenpäin ja käyttänyt vääriä lounasseteleitä eri ravintoloissa maksuvälineenä. A:n kotoa oli löytynyt 238 kappaletta käyttämättömiä lounasseteleitä. A oli siis

hankkiakseen itselleen oikeudetonta taloudellista hyötyä, käyttänyt maksuvälinettä ilman laillista oikeutta tai luovuttanut maksuvälineen toiselle saattaakseen sen ilman laillista oikeutta käytettäväksi. Syyksi luettu rikos oli maksuvälinepetos. (KKO 2019:44.)

Rikoslain 37 luvun 8§:n kolmannessa kohdassa maksuvälineeseen liittyvää dataa syöttämällä, muuttamalla, tuhoamalla, vahingoittamalla, siirtämällä tai poistamalla taikka tietojärjestelmän toimintaan muuten puuttumalla saa aikaan rahan tai rahan arvon siirron lopputuloksen vääristymisen ja siten aiheuttaa toiselle taloudellista vahinkoa, on tuomittava maksuvälinepetoksesta. Tämän kohdan mukainen rikoksen yritys on rangaistavaa.

Maksuvälinepetoksesta tuomitaan myös se, joka tilin katteen tai sovitun enimmäisluottorajan ylittäen väärinkäyttää rikoslain 37 luvun 8§:n ensimmäisessä momentissa tarkoitettua maksuvälinettä ja siten aiheuttaa toiselle taloudellista vahinkoa, jollei hänellä maksuvälinettä käyttäessään ollut aikomus viipymättä korvata vahinko. Maksuvälinepetoksesta voidaan tuomita sakkoa tai vankeutta enintään kaksi vuotta.

2.4 Törkeä- ja lievä maksuvälinepetos

Rikoslain 37 luvun 9 §:ssä säädetään törkeästä maksuvälinepetoksesta, jonka mukaan törkeästä maksuvälinepetoksesta on kyse, jos maksuvälinepetoksella aiheutetaan huomattavaa tai erityisen tuntuvaa vahinkoa. Rikos tehdään erityisen suunnitelmallisesti tai rikos tehdään osana järjestäytyneen rikollisryhmän toimintaa. Koventamisperusteista ja järjestäytyneestä rikollisuudesta säädetään rikoslain 6 luvun 5 §:n 2 momentissa.

Maksuvälinepetoksen tulee olla kokonaisuutena arvostellen törkeä. Törkeästä maksuvälinepetoksesta on rikoksen tekijä tuomittava vähintään neljäksi kuukaudeksi ja enintään viideksi vuodeksi vankeuteen. Törkeän maksuvälinepetoksen yritykseen sovelletaan vastaavasti, mitä 8 §:ssä säädetään yrityksestä.

Lievästä maksuvälinepetoksesta säädetään rikoslain 37 luvun 10 §:ssä ja sen mukaan: Jos maksuvälinepetos, huomioon ottaen tavoitellun hyödyn tai aiheutetun vahingon määrä taikka muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen, rikoksentekijä on tuomittava lievästä maksuvälinepetoksesta sakkoon. Rikoslain 37 luvun 10 §:n mukaista lievää maksuvälinepetoksen yritystä ei ole säädetty rangaistavaksi.

Rikoslain 5 luvun 1 §:n mukaan rikoksen yrityksestä voidaan rangaista vain, jos tekijän yritys on tahallinen ja kyseinen rikos on säädetty rangaistavaksi rikosta koskevassa säännöksessä. Rikok-

sen katsotaan siirtyneen yritysvaiheeseen, kun tekijä on aloittanut rikoksen toimeenpanon ja aiheuttanut vaaran rikoksen täyttymisestä. Vaikka vaaraa ei syntyisikään, rikoksen katsotaan olevan yritys, jos vaaran puuttuminen johtuu pelkästään satunnaisista syistä. (HE 52/2021 vp, 20.)

Maksuvälinepetoksen tunnusmerkistöä on korkein oikeus 1999 käsitellyt seuraavassa oikeustapauksessa. Kyseisessä oikeustapauksessa A oli yrittänyt hankkia itselleen oikeudetonta taloudellista hyötyä. A oli B:ltä anastamallaan pankkikortilla eli ilman sen laillisen haltijan lupaa yrittänyt nostaa pankkiautomaatilta käteistä siinä onnistumatta. Kortti oli jäänyt automaattiin, koska syötetty tunnusluku oli ollut väärä. Syyttäjä vaati tapauksessa A:lle rangaistusta maksuvälinepetoksesta. Korkeimmassa oikeudessa katsottiin, että A oli yrittänyt nostaa anastamallaan pankkikortilla rahaa pankkiautomaatista ja käyttänyt väärää tunnuslukua yrityksessään onnistumatta ja pankkikortti oli jäänyt automaattiin. Hänen katsottiin syyllistyneen täytettyyn maksuvälinepetokseen. Tapauksessa kortinhaltijan tilillä olleiden varojen määrästä ei ole esitetty selvitystä, A:n rikos on kokonaisuutena arvostellen vähäinen. Tuomiosta ilmenevissä olosuhteissa tekoa pidettiin lievänä maksuvälinepetoksena. (KKO: 1999:110.)

2.5 Maksuvälinepetoksen valmistelu

Rikoslain 37 luvun 11 §:ssä säädetään maksuvälinepetoksen valmistelusta, jonka tekijä voidaan tuomita sakkoon tai vankeuteen enintään kahdeksi vuodeksi. Pykälän ensimmäisen kohdan mukaan henkilö, joka pitää hallussaan, valmistaa, hankkii, tuo maahan, myy kuljettaa, levittää tai pitää saatavilla maksuvälinelomakkeen tai erityisesti maksuvälinelomakkeen valmistamiseen soveltuvan välineen tai tarvikkeen on tuomittava maksuvälinepetoksen valmistelusta.

Rikoslain 37 luvun 11§:n toisen kohdan mukaan henkilö, joka valmistaa, hankkii, tuo maahan, pitää hallussaan, myy, kuljettaa, levittää, luovuttaa, vie maasta tai pitää saatavilla erityisesti maksuvälineen väärentämiseen soveltuvan välineen tai tarvikkeen taikka erityisesti tietoverkoissa tapahtuvaan maksuliikenteeseen soveltuvan välineen, tarvikkeen, laitteen, tallenteen, tietokoneohjelman tai ohjelmakäskyjen sarjan on tuomittava maksuvälinepetoksen valmistelusta.

Maksuvälinepetoksen valmistelu edellyttää tekojen suorittamista maksuvälinepetosrikoksen toteuttamiseksi. Tunnusmerkistö kattaa tilanteet, joissa henkilö valmistelee maksuvälinepetoksen tekemistä ja syyllistyy siten mainittujen laitteiden valmistamiseen, maahantuontiin, hankintaan, hallussapitoon, myyntiin tai niiden luovuttamiseen. (HE 52/2021 vp, 18.)

Maksuvälinepetoksen valmistelu pykälä on muuttunut rikoslain uudistuksen, myötä aiemmin maksuvälinepetoksen valmistelusta voitiin tuomita sakkoon tai vankeuteen yhdeksi vuodeksi (HE 38/1997). Pykälän 1 kohta koskee nykyään maksuvälinelomakkeen valmistamista, maahan tuontia,

hankkimista, vastaanottamista tai hallussa pitämistä maksuvälinepetoksen tekemistä varten. Kohdan tekotapoihin on lisätty uusina tekotapoina myyminen, kuljettaminen, levittäminen ja saatavilla pitäminen (HE 52/2021 vp, 39).

Pykälän 2 kohdassa säädetään nykyisin myös tietoverkoissa tapahtuvaan maksuliikenteeseen soveltuvan tallenteeseen, ohjelmistoon, välineeseen tai tarvikkeeseen liittyvistä teoista maksuvälinerikoksen tekemistä varten. Kohdassa mainittuja termejä on päivitetty siten, että kohdassa säädetään erityisesti tietoverkoissa tapahtuvaan maksuliikenteeseen soveltuvasta välineestä, tarvikkeesta, laitteesta, tallenteesta, tietokoneohjelmasta tai ohjelmakäskyjen sarjasta. Maksuvälineiden väärentämiseen soveltuvien välineisiin ja tarvikkeisiin ei enää sovelleta väärennysaineiston hallussapitoa koskevaa säännöstä, vaan maksuvälinepetoksen valmistelua koskevaa 2 kohdan mukaista säännöstä. (HE 52/2021 vp, 39.)

2.6 Maksuvälinepetosten määrästä

Viime vuosina nettihuijaukset ja tietojenkalastelu ovat kasvaneet huomattavasti ympäri maailmaa. Rikolliset käyttävät hyväkseen internetin monipuolisia mahdollisuuksia ja ihmisten luottamusta verkossa tapahtuvaan viestintään ja asioiden hoitamiseen. Sosiaalisen median alustat, mobiilisovellukset ja muut teknologiset innovaatiot tarjoavat tehokkaita työkaluja tietojen kalasteluun. Lisäksi internet mahdollistaa kansainvälisen toiminnan, mikä tekee rikollisten kiinnijäämisestä vaikeampaa. Anonymiteetti verkossa antaa rikollisille rohkeutta toimia ilman pelkoa seuraamuksista. Verkossa avusteisissa maksuvälinepetoksissa ja tietojenkalastelulla voi olla suuria taloudellisia hyötyjä rikollisille. He voivat varastaa rahaa suoraan uhrin tileiltä tai myydä varastettuja henkilötietoja eteenpäin rikollisille. (Thomas ym. 2022, 212.)

Suomessa nettipetosten kasvu on ollut huomattavaa 2010-luvulla, ja se on muodostunut merkittäväksi haasteeksi niin yksilöille kuin yrityksillekin. Tämä kehitys on seurausta digitaalisen teknologian ja internetin laajamittaisesta käytön lisääntymisestä kaikilla elämänalueilla. Esimerkiksi verkkokaupankäynnin suosion kasvu, sosiaalisen median käytön lisääntyminen sekä uusien maksutapojen ja digitaalisten palveluiden kehittyminen ovat luoneet otollisen maaperän erilaisille petoksille ja huijauksille. (Lehtonen 2016.)

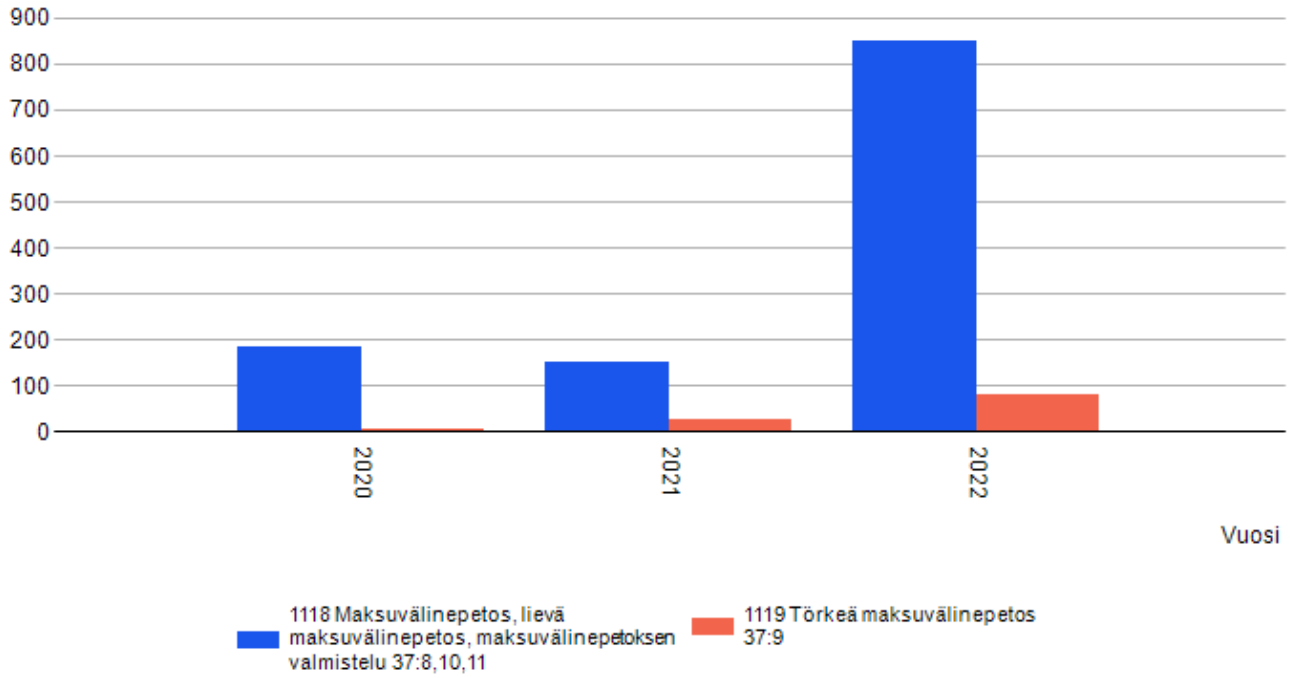
Viimeisen kymmenen vuoden aikana viranomaisten tietoon tulleiden maksuvälinepetosten määrä on vaihdellut merkittävästi vuosittain. Vuosina 2015 ja 2016 poliisille ilmoitettujen rikosten määrä kasvoi huomattavasti, vuonna 2015 luku oli 11 000 ja vuonna 2016 peräti 15 143 ilmoitettua rikosta. Kuitenkin vuonna 2017 ilmoitettujen maksuvälinepetosten määrä väheni dramaattisesti 56 % edellisvuoteen verrattuna, laskien 6 793 ilmoitukseen. On huomioitava, että ulkomailla tehtyjen maksuvälinepetosten osuus oli tuolloin merkittävä, sillä esimerkiksi vuonna 2016 peräti 42 % mak-

suvälinepetoksista tehtiin ulkomailla. Tällaiset ulkomailla tehdyt petokset voivat sisältää luottokorttitietojen kopiointia tai väärille teille päätyneiden korttitietojen käyttöä tietomurron seurauksena. (HE 52/2021 vp, 35.)

Vuosien 2018–2019 aikana viranomaisten tietoon tuli hieman yli 6 000 maksuvälinepetosta. Vuonna 2019 näistä tapauksista 4 468 oli perusmuotoisia maksuvälinepetoksia, 219 törkeitä maksuvälinepetoksia, 1 649 lieviä maksuvälinepetoksia ja 14 maksuvälinepetoksen valmistelua. (HE 52/2021 vp, 35.)

Maksuvälinepetoksia tehdään nykypäivänä tietoverkko avusteisesti enemmän, kuin koskaan aikaisemmin. Kuviossa 2 voidaan havaita lukumäärinä, kuinka paljon maksuvälinepetoksia on tapahtunut kolmen vuoden ajanjaksolla ja tarkasteltavina vuosina ovat 2020–2022. Sininen pylväs sisältää maksuvälinepetoksen valmistelun, maksuvälinepetoksen ja sen lievän tekomuodon. Oranssi pylväs kuvastaa törkeän maksuvälinepetoksen lukumäärää. Kuviossa on lukumäärinä kaikki tietoverkko avusteiset viranomaisten tietoon tulleet maksuvälinepetokset. Kuviosta voidaan huomata, että 2020 ja 2021 vuosina perusmuotoisia ym. maksuvälinepetoksia on tapahtunut alle 200 kappaletta vuositasolla, kun 2022 vuonna on havaittavissa selkeä piikki, jolloin viranomaisten tietoon on tullut yli 800 kappaletta vuositasolla.

Törkeitä maksuvälinepetoksia on tullut viranomaisten tietoon reilusti vähemmän, kun perusmuotoisia, mutta nekin noudattavat samaa kaavaa määrän puolesta. Vuodesta 2020 voidaan sanoa, että määrä on reilusti alle 10 ja 2021 vuonna törkeitä maksuvälinepetoksia on tullut viranomaisten tietoon, vain kourallinen. Vuonna 2023 törkeän tekomuodon määrä lähentelee jo 100 kappaletta vuositasolla. (Kuvio 2.)



KUVIO 2. Rikos- ja pakkokeinotilasto. Viranomaisten tietoon tulleet rikokset. Tietoverkkoa hyväksikäyttäen tehty maksuvälinepetos, lievä maksuvälinepetos, maksuvälinepetoksen valmistelu ja törkeä maksuvälinepetos (Tilastokeskus 2024).

Verkkoympäristöllä on petosten määrää lisäävä vaikutus, syynä tähän on verkkoasioinnin lisääntynyt käyttö tavaroiden ostamisessa ja pankkiasioiden hoitamisessa. Lisäksi potentiaalisten erehdytettävien suuri määrä ja verkossa tapahtuneen rikoksen matala kiinnijäämisriski. (Piira, 2022, 19.)

3 MAKSUVÄLINEISTÄ

Kappaleessa käydään läpi maksuvälineet, jotka ovat määritelty rikoslain 37 luvun mukaan, jotka siis sisältävät yksilöiviä tunnistetietoja, kuten maksukortin magneettijuova, etupuolella oleva mikrosiru tai kortin numero. Maksuvälineet, jotka sisältävät tunnistetietoja ovat oleellinen osa tätä opinnäytetyötä, kuten jo aiemmin mainitsin työssäni, jotta maksuvälinepetos voi tapahtua täytyy toisen esimerkiksi käyttää maksuvälinettä ilman sen laillisen haltijan lupaa. Tämän takia ei käteistä maksuvälineenä käydä läpi. Shekin ja tallenteen käyttö maksuvälineenä jää, myös tämän tutkimuksen ulkopuolelle, sillä sen käyttö on Suomessa hyvin vähäistä (HE 52/2021 vp, 38).

3.1 Maksuvälineiden kehittyminen

Maksukorttien käyttö yleistyi Suomessa 1960-luvulla, ja ensimmäinen maksukortti oli nimeltään Luottokunnan OK-kortti. Magneettijuova lisättiin maksukortteihin vuonna 1970, mikä teki korttimaksuista sähköisiä. Magneettijuovassa oli kaikki tarvittavat tiedot maksun vahvistamiseen, kuten kortinhaltijan nimi, kortin numero ja voimassaoloaika. (Mobile transaction, 2020.)

Visa on Suomessa tunnetuin luottokortti ja samalla maailman johtava kansainvälinen luottoyhtiö. Visa-kortit tulivat käyttöön vuonna 1976, ja ensimmäiset kortit saapuivat Suomeen 1980-luvun alussa. Aluksi käytössä olivat niin kutsutut maksuaikakortit, ja vasta 2000-luvulla niihin oli mahdollista liittää luotto-ominaisuus. (Yle 2010.)

Ensimmäiset sirukortit otettiin käyttöön Suomessa vasta vuonna 1997. Sirun ja PIN-koodin käyttöönotto merkittävästi paransi maksukorttien turvallisuutta, koska sirukorttia käytettäessä ei enää ollut mahdollista väärentää allekirjoituksia, toisin kuin aiemmin. Suomeen lähimaksu tuli ensimmäistä kertaa vuonna 2013, ja viimeisten muutaman vuoden aikana sen suosio on kasvanut huomattavasti. Alussa lähimaksulla pystyi maksamaan vain 25 euron summiin asti. (Mobile transaction, 2020.)

Biometrinen tunnistautuminen hyödyntää sormenjälkitunnistusta maksukortin käyttäjän henkilöllisyyden varmistamiseen. Tämä lisää maksutapahtuman turvallisuutta ja saattaa tulevaisuudessa korvata perinteiset maksukortit. Mastercard on parhaillaan testaamassa sormenjälkiteknologiaa hyödyntäviä kortteja. Tulevaisuus maksuvälineiden ja maksupäätteiden osalta herättää paljon kysymyksiä seuraavan 10 vuoden aikana. Vaihtoehtoja on lukuisia ja niitä tulee jatkuvan kehityksen myötä lisää. Maksuteknologian kehitys on nopeaa ja monimuotoista tällä hetkellä. On kuitenkin selvää, että tulevaisuudessa kosketusnäytöt ja langattomat laitteet todennäköisesti valtaavat alaa, tarjoten entistä kehittyneempiä vaihtoehtoja verrattuna aikaisempiin "korttihöylä" -maksupäätteisiin. (Mobile transaction, 2020.)

3.2 Maksukortit

Maksukortit ovat yleisimpiä sähköisiä maksuvälineitä, mutta lainsäädäntömme ei aina pysy kehityksen tahdissa. Erilaiset maksukortit ovat hyvä esimerkki tästä. Vaikka erilaisia korttimuotoisia maksuvälineitä käytetään laajasti Suomessa, vain kuluttajien käytössä olevat luottokortit ovat säädetyn lain piirissä. Lain soveltaminen rajoittuu lähinnä kortin oikeudettomaan käyttöön, josta seuraa rangaistus. Muut luottokortteihin liittyvät erityiset oikeuskysymykset jäävät lain ulkopuolelle. Maksukortteja on kuitenkin monenlaisia, ja ne tarjoavat erilaisia ominaisuuksia ja etuja käyttäjilleen. (Aurejärvi & Hemmo 2004, 321.)

Luottokortti mahdollistaa maksujen suorittamisen erilaisille palveluille ja tuotteille, kunhan myyjä hyväksyy sen maksuvälineenä. Luottokortin keskeinen toimintaperiaate on toimia maksuvälineenä sekä antaa käyttäjälle maksuaikaa luoton muodossa. Sen oikeudelliset ominaispiirteet liittyvät maksuvälineen rooliin ja mahdolliseen luottokorttivelkaan. Kortin käyttöehdoissa määritellään maksuaika, joka annetaan kortin haltijalle. Tämä erottaa luottokortin tavallisesta pankkikortista, jossa maksu veloitetaan välittömästi tililtä. (Aurejärvi & Hemmo 2004, 323–324.)

Vuonna 2010 Europol arvioi, että maksukorttirikollisuus aiheuttaa noin 1,5 miljardin euron tappiot Euroopan unionin alueella vuosittain. Tarkkaa kokonaistappioiden määrää on vaikea määrittää, sillä merkittävä osa maksukorttirikollisuudesta jää piilorikollisuuden piiriin. Lisäksi EAST (European ATM Security Team) ilmoitti, että käteisautomaatteihin kohdistuva järjestäytynyt rikollisuus aiheuttaa noin 425 miljoonan euron tappiot vuosittain. Tähän lukuun eivät sisälly esimerkiksi korttien uusimisesta aiheutuvat kustannukset. (HE 52/2021 vp, 35.)

Maksaminen ja maksu ovat kehittyneet paljon viimeisien vuosien aikana ja tarjolla on paljon erilaisia tapoja maksaa. Maksukortin tiedot voi nykyään syöttää, myös IOS 11 käyttöjärjestelmässä ja sitä uudemmissa Apple Wallettiin, joihin lisättyjä kortteja voi käyttää mobiilimaksamiseen Apple Payn kautta. Apple Pay julkaistiin Suomessa vuonna 2017, joten mobiilimaksutapa on vielä tuore keksintö. Apple Pay on tänä päivänä monikäyttöinen ja sitä voi hyödyntää verkko ostosten tekemisessä tai kaupan kassalla, Applen älykellon kautta (Apple 2024). Apple Payn käyttö on ollut nousussa ja se on omalta osaltaan nopeuttanut ja helpottanut maksamista, vaikka maksutapahtuma tavallisella sirukortilla on ollut nopeaa jo pitkän aikaa. Turvallisuuden näkökulmasta Apple Pay poistaa ainakin sen vaihtoehdon, että joku varastaisi maksukortin ja urkkisi PIN-koodin kaupan kassalla. Toki on mahdollista, että puhelin tulee anastetuksi ja voro on tietoinen puhelimen pääsykoodista, jolloin maksutapahtuman tekeminen Apple Payta käyttäen on vielä mahdollista, mutta uusimmat teknologiat sormenjälkitunnistus ja Face ID:n käyttö maksutapahtuman yhteydessä syrjäyttävät nämäkin tavat.

Android käyttöjärjestelmälle on vastaava mobiilimaksamiseen tarkoitettu Google Pay. Google Pay, mobiilimaksupalvelu, otettiin käyttöön Suomessa marraskuussa 2018. Sovellus on saatavilla vähintään Android 5.0 -käyttöjärjestelmää käyttäville älypuhelimille ja sen käyttö edellyttää Google-tiliä, jonka avulla käyttäjä voi hallinnoida maksukorttejaan. Google Pay on ilmainen sovellus ja se voidaan ladata Android-puhelinten Google Play -kaupasta. Lisäksi se on saatavilla myös Applen laitteille App Storesta. Apple, sekä androidia käyttävät elektroniikka merkit tarjoavat käyttäjille puhelimen välityksellä maksamisen lisäksi älykelloja ja sormuksia, joihin voi liittää maksutoiminnon.

3.3 Virtuaalivaluutta

Nykyisin voidaan lähtökohtaisesti arvioida, että maksuvälineen määritelmä kattaa myös sähköisen rahan ja virtuaalivaluutan, edellyttäen että jälkimmäistä käytetään maksuliikenteessä. (HE 52/2021 vp, 46.) Virtuaalivaluutat ovat digitaalisia arvon säilyttäjiä, jotka eivät ole peräisin keskuspankilta tai viranomaisilta eivätkä ole niiden takaamia. Ne eivät välttämättä ole sidoksissa viralliseen maksuvälineeseen, mutta niitä hyväksytään maksuvälineenä sekä yksityishenkilöiden että oikeushenkilöiden keskuudessa. Virtuaalivaluuttoja voidaan siirtää, säilyttää ja myydä sähköisessä muodossa. (HE 52/2021 vp, 6.)

Yksi tunnetuimmista virtuaalivaluutoista on Bitcoin. Virtuaalivaluutat, kuten Bitcoin, voidaan nähdä varallisuuden muotoina, mutta niiden arvo perustuu toimiviin markkinoihin. Viime aikoina termi "kryptovarat" on alkanut yleistyä puhuttaessa virtuaalivaluutoista ja kryptovaluutoista. (Suomen Pankki, 2018.)

Bitcoin on digitaalinen valuutta, joka kehitettiin vuonna 2008 vaihtoehdoksi valtioiden ja keskuspankkien hallinnoimille perinteisille valuutoille. Se ei ole fyysisessä muodossa, vaan toimii pääasiassa internetissä käytettävänä virtuaalirahana. Bitcoin toimii hajautetussa vertaisverkossa, mikä tarkoittaa, ettei sille ole yhtä keskitettyä hallitsijaa tai toimijaa. Sen arvo määräytyy täysin kysynnän ja tarjonnan perusteella ilman ulkopuolista, keskuspankkien tai muiden tahojen säätelyä. (Pagliery 2014, 30.)

Bitcoin on hajautetun yhteisön ylläpitämä digitaalinen valuutta, joka perustuu kryptografiaan ja toimii lohkoketjun avulla. Lohkoketju tallentaa luotettavasti kaikkien tapahtumien tiedot ja varmistaa niiden oikeellisuuden matkan varrella tapahtuvien varmennusten avulla. Jokainen siirto noudattaa ennalta määritettyjä sääntöjä, jotka turvaavat käyttäjien toiminnan ja lisäävät verkoston läpinäkyvyyttä. Lohkoketjussa jokainen transaktio on täysin jäljitettävissä aina valuutan luomishetkestä asti, mikä lisää sen läpinäkyvyyttä. (Rosenberg 2021.)

Nykypäivänä viranomaiset käsittelevät virtuaalisia varoja yhä enemmän oikeudellisesta näkökulmasta ja samalla tavalla kuin muita omaisuuseriä, mikä helpottaa niiden takavarikointia. Virtuaaliset varat tulevat koko ajan kansalaisille, sekä viranomaisille tutummiksi. Vastaavasti rikollisten keskuudessa virtuaalivaluutat ovat arkipäivää ja rikolliset etsivät jatkuvasti uusia tapoja tulonlähteiden löytämiseksi, joista yksi kryptovaluutan louhinta. Kryptovaluutan louhintaa voi, myös harjoittaa laillisesti, mutta rikolliset ovat kehittäneet louhintaan koko ajan parempia ja pidemmälle vietyjä tapoja tietämättömien uhrien infrastruktuurissa. (Enisa 2023.)

Virtuaalivaluutan yleistyminen ja sen aluevaltaaminen maksuvälineenä on ottanut jo ensiaskeleet. Siihen pisteeseen ei ole vielä päästy, että virtuaalivaroilla voisit maksaa, jokapäiväisiä ostoksia vaivattomasti, mutta käytännössä sekin on jo mahdollista, sillä Suomestakin löytyy jo useita virtuaalivarojen nostoon tarkoitettuja automaatteja eli bittimaatti. Bittimaatista voit nostaa virtuaalisia varoja käteiseksi ja samalla, myös ostaa tutuimpia kryptovaluuttoja, kuten bitcoinia tai ethereumia. (Bittimaatti 2023.)

4 MAKSUVÄLINEPETOSTEN TEKOTAVOISTA

Useimmissa maksukorteissa on vähintään kaksi teknistä sovellusta, jotka välittävät kortin yksilöivää tietoa maksutapahtumaan: magneettijuova kortin takapuolella ja mikrosiru kortin etupuolella. Kortin numero, joka aiemmin oli kohokirjoituksella kortin etupuolella, ei enää ole uusimmissa korteissa. Magneettijuova on vanhentunut ja haavoittuva tekniikka, kun taas mikrosirua ei ole toistaiseksi onnistuttu kopioimaan. Yleisin tapa väärinkäyttää maksukorttia on urkkia PIN-koodi jollain tavalla, esimerkiksi kassalla tai automaatilla, ja sen jälkeen anastaa fyysisesti kortti ja nostaa käteistä kortilla. (HE 52/2021 vp, 34.)

Puolustus erilaisia kyberrikoksia vastaan on yhtä vahva, kuin sen heikoin lenkki, mikä edelleen on ihmisen toimesta suoritettu valvonta. Kalasteluviestit, haitalliset dokumenttitiedostot, sosiaalisen manipuloinnin tekniikat ja päivittämättömät ohjelmisto- ja laitteistot ovat yleisimpiä tapoja, joilla rikolliset tunkeutuvat uhriensa järjestelmiin. (IOCTA 2023.)

4.1 Sivustoharhautus

Sivustoharhautus on huijausmenetelmä, jossa hyökkääjä pyrkii saamaan käyttäjän paljastamaan henkilökohtaisia tietojaan, kuten käyttäjätunnukset, salasanat tai maksukorttitiedot, luomalla väärennetyn verkkosivuston, joka näyttää aidoilta ja luotettavilta. Tavoitteena on harhauttaa käyttäjä antamaan arkaluonteisia tietojaan, joita sitten voidaan käyttää väärin, kuten identiteettivarkauden tai taloudellisen hyödyn tavoittelun muodossa. (Kolttola & Beuker, 2023, 106.)

Tyypillisessä sivustoharhautuksessa hyökkääjä lähettää käyttäjälle houkuttelevan sähköpostin, tekstiviestin tai sosiaalisen median viestin, jossa pyydetään klikkaamaan linkkiä ja kirjautumaan sisään tiettyyn verkkopalveluun, kuten pankkitiliin tai sähköpostiin. Linkki johtaa kuitenkin väärennetylle verkkosivustolle, joka näyttää täysin aidoilta, mutta on itse asiassa hyökkääjän hallitsema. Kun käyttäjä syöttää henkilökohtaiset tiedot väärennetylle sivustolle, ne tallentuvat hyökkääjän käyttöön. Näin hyökkääjä saa käyttöönsä arkaluonteisia tietoja, joita voidaan käyttää väärin esimerkiksi iden-

titeettivarkauden, taloudellisen petoksen tai muiden haitallisten toimien toteuttamiseen. Sivustoharhautus voi olla erittäin hankala tunnistaa, koska väärennetyt verkkosivustot voivat näyttää hyvin aidoilta ja luotettavilta. Myös ulkomailta toimivat rikolliset voivat olla osallisina näissä petoksissa. Teknologinen kehitys on mahdollistanut yhä monimutkaisemmat huijausmenetelmät, jotka voivat olla vaikeasti tunnistettavissa perinteisiksi verkkohuijauksiksi. (Kolttola & Beuker, 2023, 106.)

Englannin kielestä nimensä saanut tekniikka deepfake tarkoittaa teknologiaa, joka käyttää tekoälyohjelmistoja tekemään synteettisiä kopioita todellisten ihmisten äänistä, kuvista ja videoista. Rikollisissa toiminnoissa ja verkkopalveluissa deepfake on henkilöllisyyden väärinkäyttötekniikka, sekä tuo harhautukseen lisää luotettavuutta oli sitten kyse sivustoharhautuksesta tai verkkourkinnasta. Esimerkkinä yhdessä tapauksessa olivat rikolliset käyttäneet deepfake-äänitallennetta yrityksen toimitusjohtajan teeskentelemiseksi ja houkutellakseen siirtämään 35 miljoonaa euroa vastaava summa deepfaken avulla. Deepfake tekniikalla aiheutettujen vahinkojen torjuminen tulee olemaan äärimmäisen välttämätöntä taistelussa verkossa toimivia rikollisia vastaan. Metaversumi eli virtuaalinen todellisuus voi myös avata uusia mahdollisuuksia erilaisille petosjärjestelmille. Lisääntyneen innovatiivisten teknologioiden ja työkalujen käytön myötä rikollisille palveluille ominainen ekosysteemi todennäköisesti laajenee palvelemaan laajempaa rikollisten joukkoa, mikä mahdollistaa rikollisen toiminnan entistä useammille toimijoille ja toimii monistajana järjestäytyneelle rikollisuudelle. Sekä rikollisverkostot että yksittäiset toimijat saavat uusia ja haitallisempia tapoja uhriensa vahingoittamiseen. (IOCTA 2023.)

Deepfake ja tekoälyn käyttäminen rikollisessa toiminnassa on äärimmäisen haitallista verkkoturvallisuuden kannalta. Tekoäly helpottaa jo tällä hetkellä monia ihmisiä, niin töissä kun vapaa-ajalla. Samalla se toimii, myös rikollisessa tarkoituksessa ja tehostaa rikollisia toimintatapoja, sekä nopeuttaa niitä. Tekoälyn avulla voidaan luoda entistä todenmukaisempia valesivustoja tai huijausyrityksiä, jotka voivat tulla esille sähköpostien, tekstiviestien tai puhelinsoittojen kautta.

4.2 Tilin haltuunotto, vaaratekijä maksuvälinepetokselle

Tuoreet tutkimukset vaarantuneiden tilien ja tilitietojen kaupasta osoittavat henkilötietojen laittoman kaupan kasvavan uhan. Laajalle levinnyt vaarantuneiden tunnusten markkinat ja helposti saatavilla olevat laittomat työkalut tekevät petollisista toimijoista vähemmän riippuvaisia omasta tieto taidostaan ja erityisosaamisesta, koska jotkin tarvittavat tehtävät tilien kaappauksiin liittyen voidaan ulkoistaa tai hankkia halvalla pimeiltä markkinoilta. Tilin haltuunotot englanniksi Account takeover (ATO) altistaa uhrin suoraan maksuvälinepetoksille. (IOCTA 2023.)

Tilin kaappaus on hakkerointimuoto, joka tapahtuu, kun rikolliset pääsevät laittomasti uhriksi joutuneen henkilön verkkotilille omaksi hyödykseen. Kohdistetut tilit (kuten verkkopankki-, sähköposti- tai sosiaalisen median profiilit) ovat arvokkaita rikollisille, koska ne voivat sisältää varoja ja pääsyn

tiettyihin palveluihin tai oleellisiin yksityistietoihin, joita voidaan myydä verkossa. Tilin kaappausta pidetään nykyään melko helppona hakkerointitekniikkana, koska murtamistyökalut myydään kyberrikollisuusfoorumeilla hyvin alhaiseen hintaan. (IOCTA 2023.)

Digitaalisten sormenjälkitietojen varastaminen vaarantuneista laitteista on noussut esiin digitaalisten sormenjälkien käyttöönoton jälkeen todennusmekanismina. Tämä korostaa rikollisten sopeutumiskykyä vastatoimiin verkossa tapahtuvien petosten torjunnassa, mikä todennäköisesti jatkuu tulevaisuudessa. (IOCTA 2023.)

SIM-vaihto on toinen ATO-tekniikka, jossa rikolliset toimijat ottavat haltuunsa uhrin matkapuhelimen SIM-kortin tai hankkivat kopion SIM-kortista. Tekijät harhauttavat matkapuhelinoperaattoreita siirtämään uhrin matkapuhelinnumeron SIM-korttiin, joka heillä on hallussaan, jotta he voivat vastaanottaa saapuvia puheluita ja tekstiviestejä sekä päästä käsiksi arkaluontoisiin tietoihin. SIM-vaihtoa käytetään usein kertakäyttöisen salasanan saamiseen rahansiirtojen valtuuttamiseksi. Vuonna 2022 SIM-vaihtotapausten määrä oli vähentynyt, todennäköisesti johtuen teleoperaattoreiden toteuttamista paremmista ehkäisy- ja asiakastunnistusmekanismeista. (IOCTA 2023.)

Tilin haltuunotto, joka mielletään paremmin hakkerointina, on termi, joka viittaa tietojärjestelmien, tietokoneiden tai verkkojen luvattomaan käyttöön tai manipulointiin. Se voi kattaa laajan valikoiman toimintoja, kuten tietojen varastamisen, tietojärjestelmien vahingoittamisen tai tietojen kalastelua. Viime vuosina on havaittu, että hakkerointi on tullut entistä helpommaksi monista syistä, mikä on lisännyt sen esiintymistä ja vaikutuksia. Hakkerointi tuottaa sivurikoksena mukanaan maksuvälinepetoksia, joita voi tapahtua useita yhden tunnuksen tai tilin haltuunoton tuotoksena. Usein tämän kaltaiset maksuvälinepetokset ilmaantuvat myöhemmin uhrin tietoon, vaikka tilin haltuunotto olisi tapahtunut paljon aikaisemmin. Ominaista tilien haltuunotolle, kuten muillekin rikostyypeille on, että yksi tekijä tekee useita kertoja saman rikoksen.

Keskeinen syy hakkeroinnin helpottumiseen on teknologian kehittyminen. Kasvava digitalisaatio ja monien laitteiden ja järjestelmien yhdistyminen verkkoon ovat luoneet useita haavoittuvuuksia, joita voidaan hyödyntää hyökkäyksissä. Lisäksi avoimen lähdekoodin ohjelmistojen ja työkalujen saatavuus on lisännyt hakkerointimahdollisuuksia, koska ne tarjoavat pohjan, jota voidaan käyttää hyväksi kehittyneiden hyökkäysten suunnittelussa. Merkittävänä tekijänä voidaan pitää hakkeroinnin helpottumiselle jatkuvasti kasvava tietoisuus ja taitotaso hakkerointitekniikoista, sekä halvat työkalut hakkeroinnille. Internetissä on runsaasti oppimateriaalia ja ohjeita, jotka opettavat erilaisia hakkerointimenetelmiä. Tämä tarkoittaa sitä, että kynnys päästä mukaan hakkerointiin on alhainen, ja uusien tekniikoiden oppiminen on helpompaa kuin koskaan ennen.

Hakkeroinnin sivutuotoksena pimeille markkinoille tulee myyntiin maksukorttien tietoja, henkilötunnuksia tai erilaisten rahallista arvoa säilyttävien tilien tunnuksia, joita myydään eteenpäin. Hakkerointi ei ole ainoa tapa, jonka sivutuotoksena markkinoille saapuu henkilötunnuksia ja muita tilitietoja. Yksi tallainen ilmiö on jatkuvasti kasvanut verkkokauppahuijaus. Kaikki nämä tuottavat runsaasti uusia maksuvälinepetoksia.

4.3 Skimming ja shimming

Identiteettiä määrittävät paitsi henkilötiedot, myös erilaiset tunnisteet, jotka tunnistavat käyttäjän tai oikeuden tietoon tai palveluun pääsyyn. Tällaisia tunnisteita ovat esimerkiksi korttinumerot, tilitiedot ja käyttäjätunnukset. (Kangasniemi, 2012, 225.)

Maksukorttien magneettinauhoja voidaan kopioida erityisillä välineillä, jotka on suunniteltu tähän tarkoitukseen, mikä tunnetaan nimellä skimmaus. Skimmaus tulee englannin sanasta "skimming", joka viittaa luottokortin magneettinauhan kopioimiseen ja siihen, että kortinlukijan lukupää liukuu pitkin magneettinauhaa lukiessaan nauhalla olevaa korttidataa. Rikolliset asentavat skimmauslaitteita etenkin vilkkailla paikoilla sijaitseviin käteisautomaatteihin tai miehittämättömien polttoainejakelupisteiden maksukorttiautomaatteihin. Skimmauslaitteeseen tallennetuilla tiedoilla tekijät ovat voineet valmistaa väärennettyjä korttikopioita, joilla on tehty käteisnostoja ulkomailla, etenkin EU-alueen ulkopuolella. Skimmauslaitteiden suunnittelu ja valmistus edustavat ammattimaista rikollista toimintaa. Euroopan unionin alueella skimmaus on laajassa mittakaavassa vähenemässä, mikä johtuu pääosin Euroopassa käyttöön otettujen sirukorttien ja -automaattien parantuneesta turvallisuudesta. (HE 52/2021 vp, 34.)

Skimmaus ei ole uusi ilmiö Suomessa, vaan sitä on esiintynyt eri aikoina ja poliisin tietojärjestelmissä on dokumentoitu skimmaustapauksia jo vuodesta 2008 lähtien. Skimmauksessa käytetään erillistä laitetta, skimmeriä, joka asennetaan käteis- ja maksuautomaatteihin magneettijuovan tietojen kopioimiseksi maksukorteista. Rikolliset keräävät kortin tietoja ja sitä kautta pystyvät toteuttamaan identiteettivarkauksia tai tekemään luvattomia ostoksia kortinhaltijan nimissä. Skimmereitä käytetään usein osana erilaisia maksuvälinepetoksia. Skimmereitä on monenlaisia, ja niitä suunnitellaan sopimaan erilaisiin pankki- ja maksuautomaattimalleihin. Skimmerien suunnittelijat valmistavat laitteet ammattimaisesti alusta loppuun ja toimittavat ne henkilöille, jotka asentavat ne automaatteihin. Jotkut skimmerit on valmistettu 3D-tulostimilla. Skimmauksen taustalla on ammattimainen rikollistoiminta. (Kunelius, 2017.)

Fyysinen kortin skimmaus ei ole EU:n alueella suuri uhkatekijä ja skimmausta on havaittu jo pidemmän aikaan. Nykyään maksukorttien siruihin kohdistuvia relehyökkäyksiä (shimming) havaitaan yhä enenevissä määrin. Samankaltaisesti kuin skimmaus, shimming on tiedon väärinkäyttöä ja/tai

manipulointia kortin ja kortinlukijan siruliitännän välillä kulkevassa tiedossa. Viime vuosina maksukorttien siruihin kohdistuvista relehyökkäyksistä on raportoitu yhä enemmän EU:ssa. Relehyökkäyksessä hyökkääjä sieppaa viestinnän kahden osapuolen välillä ja välittää sen sitten toiselle laitteelle. Hyökkääjän ei tarvitse aloittaa mitään viestintää lähettäjän ja vastaanottajan välillä. (IOCTA 2023.)

4.4 Haittaohjelmista

Haittaohjelmat internetissä voivat kopioida maksukorttien numeroita ja muita tunnistetietoja. Suurin osa maksukorttidatan väärinkäytöksistä tapahtuu haittaohjelmien avulla tai suorilla tunkeutumisilla, kuten hakkeroinnilla, joka kohdistuu palvelimiin, joissa säilytetään tietoja. Erityisesti kassapalvelimet ja erilaiset nettipalvelujen käyttäjätilit ovat olleet viime vuosina rikollisten kohteena. Kun tunnistetiedot on saatu haltuun, niitä voidaan käyttää tilaamaan helposti muunnettavaa tavaraa verkkokaupoista tai esimerkiksi lentolippuja. Lisäksi mobiililaitteiden SIM-korttitietojen kaappaus on yleistynyt, kun pankkiasiointi on siirtynyt entistä enemmän mobiiliverkkoihin. (HE 52/2021 vp, 34.)

Haittaohjelmiin perustuvat kyberhyökkäykset ovat edelleen merkittävä uhka ja koostuvat useista eri haittaohjelmatyypeistä ja tunkeutumistekniikoista, jotka käytetään yhdessä eri hyökkäysvaiheissa. Haittaohjelmiin perustuvat hyökkäykset jaetaan yleensä niiden lopullisen vaikutuksen perusteella. On tärkeää huomata, että riippumatta lopputuloksesta, samat tunkeutumismallit voivat johtaa useisiin eri hyväksikäyttömuotoihin riippuen hyökkäyksen tavoitteesta. Tilanteessa voi olla kyse tietojen varastamisesta, vakoilusta tai tietojen myymisestä. (IOCTA 2023.)

Rikolliset käyttävät kalastelupalveluita levittääkseen sähköposteja, jotka sisältävät asiakirjoja (esim. Excel, Word) sisältäviä haitallisia makroja eli sarja komentoja, jotka tietokone suorittaa käyttäjän puolesta tai tartunnan saaneita pakkaustiedostoja (esim. Zip, RAR) tai URL-osoitteita, jotka johtavat verkkosivuille, jotka käynnistävät haittaohjelman latauksen. Näihin lähteisiin vuorovaikutuksessa usein johtaa dropperin esiintymiseen uhrin järjestelmässä. Dropperilla tarkoitetaan virtuaalista laatikkoa, joka kätkee sisäänsä haittaohjelma komponentteja ja varmistaa niiden asennuksen järjestelmään. Erään tutkimuksen mukaan rikolliset ovat siirtäneet mieltymyksensä haitallisten makrojen käytöstä pakkaustiedostoja suosiviksi sen jälkeen, kun Microsoft esti makrot, jotka toimitetaan Internetin yli niiden sovelluksissa. Haittaohjelmien useimmiten käytetty pääjakelukanava on sähköpostikampanjat. (IOCTA 2023.)

Uhrit voivat myös saada droppereita tartunnaksi internetin hakukoneiden kautta, missä käyttäjät houkutellaan hakukoneoptimoinnin avulla lataamaan haittaohjelma, joka on naamioitu lailliseksi ohjelmaksi tai työkaluksi. Joissakin tapauksissa rikolliset käyttävät hakukoneiden mainostyökaluja ohjaamaan käyttäjiä verkkosivuille, jotka naamioituvat suosittujen ohjelmistojen lataussivustoiksi,

mutta todellisuudessa ne toimittavat haittaohjelman uhrin järjestelmään. Sama pätee, myös älylaitteisiin, joihin haittaohjelmat pääsevät sovelluskauppojen sovelluksien kautta, jotka sisältävät haittaohjelmia. Haittaohjelmilla voi olla monta tarkoitusta, mutta yksi keskeisimmistä tavoitteista on usein taloudellisen hyödyn tavoitteleminen. Tämä voi tapahtua yksikertaisuudessaan pankkitietojen kalastelulla haittaohjelmaa hyväksi käyttämällä. (IOCTA 2023.)

Virukset, troijalaiset ja madot ovat kolme yleistä haittaohjelmien tyyppiä, jotka aiheuttavat merkittäviä uhkia tietokonejärjestelmille ja verkostoille ympäri maailmaa. Jokainen näistä haittaohjelmamuodoista toimii eri tavalla, mutta niillä kaikilla on yhteinen tavoite aiheuttaa vahinkoa tai häiriöitä digitaalisille järjestelmille. Tässä esseessä tutustumme virusten, troijalaisten ja madon ominaisuuksiin sekä niiden vaikutuksiin tietoturvaan ja ennaltaehkäisymenetelmiin. (Thomas ym. 2022, 129.)

Virukset ovat ehkä tunnetuin haittaohjelmien tyyppi. Ne ovat ohjelmia tai koodinpätkiä, jotka liittyvät itsensä laillisiin tiedostoihin tai ohjelmiin ja monistavat itsensä, kun tartunnan saanut tiedosto tai ohjelma suoritetaan. Kun virus on tartuttanut järjestelmän, se voi suorittaa erilaisia haitallisia toimintoja, kuten tiedostojen korruptoimisen tai poistamisen, arkaluontoisten tietojen varastamisen tai järjestelmän toiminnan häiritsemisen. Virukset leviävät usein tartunnan saaneiden sähköpostiliitteiden, haitallisten verkkosivustojen tai tartunnan saaneiden irrotettavien tallennuslaitteiden kautta. (Thomas ym. 2022, 131.)

Troijalaiset, jotka on nimetty kuuluisan kreikkalaisen tarun mukaan, ovat petollisia haittaohjelmia, jotka teeskentelevät olevansa laillisia ohjelmistoja tai tiedostoja houkutellakseen käyttäjiä suorittamaan ne. Toisin kuin virukset, troijalaiset eivät monistu itseään. Sen sijaan ne luottavat sosiaalisiin tekniikoihin houkutellakseen uhreja asentamaan ne. Asennuksen jälkeen troijalaiset voivat suorittaa monenlaisia haitallisia toimintoja, kuten käyttäjätunnusten varastamisen, virtuaalisten takaovien asentamisen etäkäyttöä varten tai lisähaittaohjelmien lataamisen tartunnan saaneeseen järjestelmään. Yleisiä troijalaisten jakelutapoja ovat kalastusviestit, haitalliset verkkosivustot tai niputettuna luvattoman ohjelmiston kanssa. (Thomas ym. 2022, 133.)

Madot ovat itsenäisiä haittaohjelmia, jotka monistuvat itseään ja leviävät verkostoissa ilman ihmisen väliintuloa. Toisin kuin virukset, madot eivät tarvitse kiinnittyä olemassa oleviin tiedostoihin tai ohjelmiin levitäkseen. Sen sijaan ne hyödyntävät haavoittuvuuksia verkkojen protokollissa tai käyttöjärjestelmissä levitäkseen isännästä toiseen. Kun mato tartuttaa järjestelmän, se voi kuluttaa verkkojen kaistanleveyttä, heikentää järjestelmän suorituskykyä tai toimittaa haittaohjelmien latauksia, kuten kiristyshaittaohjelmia tai bottiverkon agentteja. Madot leviävät usein suojaamattomien verkkojakojen, päivittämättömien ohjelmistohaavoittuvuuksien tai sähköpostiliitteiden kautta. (Thomas ym. 2022, 136.)

4.5 Verkkourkinta (Phishing)

Verkkourkinta ja englanninkieliseltä nimeltään tunnettu phishing on rikollisten käyttämä toimintatapa, jolla yritetään saada vastapuoli avaamaan haitallinen tiedosto tai linkki, jonka avulla rikollinen voi saada taloudellista hyötyä rahan tai tiedon muodossa. Tieto voi tarkoittaa tässä tapauksessa henkilön pankkitietoja, joiden menettäminen on kohtalokasta asianomistajan näkökulmasta. Verkkourkinta on sosiaalista manipulointia, joka voi tarkoittaa käytännössä esiintymistä tunnettuna henkilönä, yrityksenä tai yhteisönä. Verkkourkintaa voidaan kohdistaa yksittäiseen henkilöön, kuin suureen yritykseen. Tietovuodot tarjoavat rikollisille mahdollisuuden valmistaa suuriakin ja uskottavampia valheita. Verkkourkinnassa, jossa käytetään tietovuodoissa paljastunutta tietoa, kuten henkilötietoa ovat vaikeita havaita valheelliseksi tiedoksi. (Enisa 2019.)

Älypuhelinten ollessa nykyaikana arkipäivää, myös verkkourkintahyökkäykset ovat lisääntyneet 85 % puhelimiin tehdyissä hyökkäyksissä. Näissä tapauksissa urkinta tapahtuu usein tekstiviestien, muiden viestipalveluiden ja sosiaalisen median kautta. Enisa kertoo raportissaan vuodelta 2018, että 90 % toimineista haittaohjelmista ja 72 % tietomurroista on saatu aikaan verkkourkinnalla. (Enisa 2019.)

Enisan vuoden 2023 julkaisemassa raportissaan mainitaan sosiaalisen manipuloinnin kasvaneen merkittävästi tekoälyn ja sen tuomien uusien tekniikoiden yleistyessä ja verkkourkinta on silti eniten käytetty hyökkäysvektori. (Enisa 2023.)

Verkkourkinta voidaan jakaa useampiin osiin, jotka jakautuvat sen toimintaperiaatteen ja tavoitteen myötä. Yleisimmin tunnetulla verkkourkinnalla pyritään saamaan usein luottokortin tietoja tai salasanoja sähköpostien avulla käyttäen sosiaalista manipulointia hyväksi. Tämä voi tarkoittaa, esimerkiksi sähköpostia, jossa pyydetään henkilöä vahvistamaan hotellivaraus, jonka yhteydessä pyydetään antamaan luottokortin tiedot. Spear-phishing eli suomeksi "keihäänkärkikalastelu" tarkoittaa verkkourkintaa, joka on viety pidemmälle ja siinä yritetään saada tietoja yrityksiltä tai tietyiltä henkilöiltä. (Enisa 2023.)

Whaling on verkkourkinnan muoto, joka rinnastettavissa aiemmin mainittuun Spear-phishing taktiikkaan. Tätä termiä käytetään, kun verkkourkinta kohdistetaan korkeassa asemassa oleviin henkilöihin, kuten poliitikkoihin ja eri yritysten johtajiin. (Enisa 2023.)

Smishing on lyhenne sanoista 'SMS' ja 'kalastelu', ja se tapahtuu silloin, kun hyökkääjä hankkii arkaluontoisia tietoja tai houkuttelee uhrit klikkaamaan haitallisia linkkejä, jotka jaetaan tekstiviestien välityksellä. Yleinen puhelimella ja samaan toimintamalliin liittyvä uhka on vishing, joka muodostuu

sanoista phishing ja voice. Se tapahtuu, kun haitalliset toimijat käyttävät puhelimitse annettuja tietoja hyväkseen käyttäen sosiaalisen manipuloinnin tekniikoita saadakseen käyttäjiltä arkaluontoisia tietoja. (Enisa 2023.)

4.6 Lähimaksun hyväksikäyttö

Lähimaksuteknologia on noussut suosioon tarjoten kätevän ja nopean tavan suorittaa maksuja pienemmissä ostoksissa. Vaikka onkin olemassa huoli siitä, että rikolliset voisivat hyödyntää tätä tekniikkaa väärin, on tähän otettu kantaa jo vuosia aikaisemmin. (Yle 2016.)

RFID-tunnusta käyttävien tavaroiden, kuten lähimaksukorttien, passien ja puhelimien NFC-tekniikan määrä on kasvanut, samoin kuin huoli siitä, että rikolliset voisivat lukea näiden laitteiden tietoja omilla laitteillaan. Tekniikan Maailma testasi RFID-tunnusten lukemisen helppoutta vuonna 2017, ja heidän testissään paljastui, että tehokkaalla radiolaitteella varustettu rikollinen voisi lukea tietoja suoraan taskussa tai käsilaukussa olevasta pankkikortista. (Tekniikan Maailma 2017.)

Nets on maksupäätemyyntiin keskittynyt yritys ja sen kaupallinen johtaja Sami Toivonen on ottanut kantaa lähimaksun turvallisuuteen liittyvissä asioissa Ylen artikkelissa vuonna 2016. Toivosen mukaan, vaikka teoriassa on mahdollista salaa veloittaa toisen maksukortilta lähimaksua ominaisuutta käyttäen. Täytyisi kyseisessä tilanteessa maksupääte tuoda hyvin lähelle lompakkoa, jonka sisällä kortti sijaitsee. Toivosen mukaan, vaikka veloittaminen kortilta onnistuisikin olisi kiinni jääminen käytännössä taattua. Lähimaksukortilta veloittamiseen tarvitaan tietynlainen päätelaite, johon on ohjelmoitu tilitystiedot, minne rahat maksetaan. Tekijä saataisiin tietää vaivattomasti, sillä rahaliikennettä on helppo seurata päätelaitteen toimintaperiaatteen vuoksi. Muista syistä kannattaa seurailla oman pankkitilin tapahtumia Toivosen mukaan. (Yle 2016.)

Kokonaisuutena voidaan todeta, että vaikka lähimaksun hyväksikäyttö saattaa herättää huolta, sen toteuttaminen käytännössä ei ole helppoa eikä kannattavaa rikollisille. Turvallisuustoimenpiteet, tekniset haasteet ja korkea kiinnijäämisriski tekevät siitä epätodennäköisen valinnan rikollisten toiminnassa.

5 JOHTOPÄÄTÖKSET

Verkossa asioiminen on tänä päivänä olennainen osa monien ihmisten arkea. Sähköiset palvelut tarjoavat kätevän tavan hoitaa monenlaisia asioita, kuten ostoksia, pankkiasioita, terveyspalveluita ja viestintää. Vaikka verkkoasiointi tuo mukanaan lukuisia etuja, kuten nopeuden ja helppouden, se

tuo myös mukanaan riskejä, kuten tietoturvaongelmia ja identiteettivarkauksia. Siksi on ensiarvoisen tärkeää, että käyttäjät ottavat käyttöön asianmukaiset turvallisuuskäytännöt varmistaakseen turvallisen verkkoasioiden hoitamisen.

5.1 Turvallisuus asioidessa verkossa

Kehittyvät tekotavat maksuvälinepetoksissa lisääntyvät ja löytävät uusia muotoja jatkuvasti ja yksi keskeisimmistä tavoitteista maksuliikenteen turvallisuuden ja luottamuksen ylläpitämiseksi on lisätä tietoisuutta tekotavoista. Tietoisuutta tulisi lisätä monelta taholta. Kyse on kansalaistaidoista, mutta myös viranomaisten velvollisuudesta turvata luottamusta monenlaisiin arkisiin asiointiin niin viranomaispalveluissa, ja eri maksupalveluissa. Lähtökohtana on, että maksupalvelut ovat jatkossakin saavutettavia ja luotettavia kaikille. Omalla toiminnalla voitaisiin estää maksuvälinerikoksien toteutuminen tai edes niiden mahdollisuus erittäin todennäköisesti.

Kuten edellä ole todennut että, maksuvälinepetoksen rangaistavuus ei edellytä erehdyttämistä tai erehtymistä, ja että rangaistavuuteen riittää, että on ollut otettava mahdollisuus aiheuttaa taloudellista vahinkoa toiselle henkilölle. Maksuvälinepetos tapahtuu tyypillisesti niin, että tekijä käyttää maksuvälinettä ilman laillisen haltijan lupaa.

Maksuvälinepetoksissa on rikosoikeudellisesti kyse rikosoikeudellisen vastuun kohdentumisesta rikollisesta toiminnasta. Asianomistajan näkökulmasta kyse voi olla enemmän menetetyn omaisuuden takaisin saamisesta, ja usein se on ensimmäisenä mielessä asian tullessa ilmi. Tärkeätä olisi saada rikollinen ja epärehellinen toiminta lakkaamaan, usein sulkemalla omat pankki- tai luottokorttitiedot. Maksupalvelulain 53 §:n mukaan maksuvälineen haltijan on käytettävä maksuvälinettä sitä koskevien ehtojen mukaisesti. Saman lain 54 §:n mukaan haltijan on ilman aiheetonta viivytystä ilmoitettava maksuvälineen katoamisesta tai sen joutumisesta oikeudettomasti toisen haltuun.

Vakuutus- ja rahoitusneuvonta Fine tehtävänä on neuvoa mm. kuluttajia vakuutus-, pankki ja sijoitustoiminnan ongelmatilanteissa ja ratkaista niihin liittyviä valitusasioita. Fine on ratkaisussaan FINE-026772 ottanut kantaa pankin korvausvelvollisuuteen. Asiassa henkilö oli lähtenyt viettämään iltaa entuudestaan tuntemattomien henkilöiden seurassa. Aluksi oli käyty tankkaamassa uusien ystävien kanssa heidän autoansa bensa-automaatilla. Henkilön ja pankin puolesta oli asiassa yksimielisyys siitä, että tankkauksen yhteydessä oli vakoiltu pankkikortin PIN- koodi. Illan aikana oli henkilöltä varastettu pankkikortti lompakosta, ja tämän jälkeen automaattinostoina oli henkilön tililtä viety 5100 euroa. Asiassa saadun selvityksen perusteella kortin oikeudettoman käytön johtuneen siitä, että henkilö on huolimattomuudessa laiminlyönyt maksupalvelulain 53§:n ja korttiehtojen mukaisia velvollisuuksiaan tunnusluvun käyttämisen ja säilyttämisen suhteen. Pankkilautakunta katsoi asiassa olleen törkeätä huolimattomuutta, ja asiassa ei suositeltu hyvitystä. (Fime.fi.)

Toisessa ratkaisussa FINE-000793 Henkilö oli tehnyt 10 euron ostoksen pankkikortilla Tallinnalaisessa ravintolassa, ja hänen poistuessaan kortti oli tallessa. Yön aikana kortilla oli tehty tunnusluvulla hyväksytyt kahdeksan maksutapahtumaa yhteisarvoltaan 7220 euroa. Pankkilautakunta katsoi asiassa, että selvityksen perusteella maksunsaaja on tietoisesti osallistunut kortin oikeudettomaan käyttöön ja ollen tietoinen, ettei ole oikeutettu kortin käyttöön. Asiassa henkilö ei ollut maksupalvelulain 62 §:n 3 momentin mukaan vastuussa kortin oikeudettomasta käytöstä. Näin ollen maksunsaajan ei voida katsoa varmistuneen asianmukaisesti maksajan oikeudesta käyttää korttia, eikä asiakas maksupalvelulain 62 §:n 3 momentin mukaisesti vastaa kortin oikeudettomasta käytöstä, ja että pankki ottaa vastatakseen kortin oikeudettomasta käytöstä vahingot täysimääräisesti. (Fime.fi, b.)

Edellä olevat esimerkit osoittavat maksuvälineiden ja maksutapahtumien käyttöön sekä hallussapitoon liittyvän huolellisuuden tärkeyden. Huolellisuuden törkeä laiminlyönti jättää vahingon maksuvälinepetoksissa kortin haltijalle, muissa tapaukissa vahinko jää palveluntarjoajalle.

Merkittäviä verkon varjopuolia on monia, mutta kokonaisuutena tietoturvaongelmat ovat suuressa osassa. Verkossa toimivat tietojärjestelmät ovat alttiita hyökkäyksille, kuten haittaohjelmille, tietomurroille ja tietojenkalastelulle. Tietomurrot voivat johtaa arkaluonteisten tietojen vuotamiseen, mikä voi aiheuttaa taloudellista vahinkoa ja vaarantaa yksilöiden yksityisyyden. Lisäksi haittaohjelmat voivat vahingoittaa tietokoneita ja varastaa henkilökohtaisia tietoja. Toinen merkittävä varjopuoli on disinformaatio ja valeuutiset. Internet mahdollistaa nopean tiedon levittämisen, mutta samalla se tarjoaa foorumin myös virheellisen ja harhaanjohtavan tiedon levittämiselle. Internetin varjopuoliin kuuluu myös yksityisyyden menetys ja valvonta. Monet palvelut ja alustat verkossa keräävät käyttäjien henkilökohtaisia tietoja ja seuraavat heidän toimintaansa verkossa.

Käyttäjien tulisikin varmistaa, että heidän laitteensa ja ohjelmistonsa ovat ajan tasalla. Tietoturva-aukkoja ja haavoittuvuuksia voidaan hyödyntää haitallisiin tarkoituksiin, joten päivitysten ja korjausten säännöllinen asentaminen on ensisijaisen tärkeää. Lisäksi tulisi käyttää virustorjuntaohjelmistoa ja palomuuria suojautuakseen haittaohjelmilta ja muilta verkossa vaanivilta uhilta. Pankeilla on vastuu tarjotessaan verkossa palvelujaan, mutta kuluttajia on myös hyvä muistuttaa omasta vastuustaan turvallisuuskäytänteissä verkko- ja mobiilimaksamisessa. Asioitaessa verkossa, on tärkeää säilyttää terve epäluuloisuus ja pitää mielessä turvallisuuskäytänteet. On hyvä muistaa, että pankit tai viranomaiset eivät koskaan pyydä pankkitunnuksia tai maksukortin tietoja puhelimitse, sähköpostitse tai tekstiviestitse. Lisäksi on tärkeää olla varovainen linkkien klikkaamisessa. Pankkitunnuksilla ei tulisi koskaan kirjautua palveluihin viesteissä olevien linkkien kautta, sillä jopa aitojen näköiset viestit voivat johtaa valesivustoille ja johtaa verkkopankkitunnusten väärinkäyttöön. Riskiä verkkopankkitunnusten väärinkäytöstä voi pienentää käyttämällä vahvan tunnistamisen välineitä,

kuten mobiili- tai kansalaisvarmennetta, viranomaisten palveluihin tunnistautuessa. (Finanssivalvonta, 2024.)

Tietoisuus huijausyrityksistä ja huijausviesteistä on tärkeää. Käyttäjien tulisi olla varovaisia avatessaan tuntemattomilta lähettämiä sähköposteja ja linkkejä, ja heidän tulisi välttää antamasta henkilökohtaisia tai taloudellisia tietojaan epäilyttäville verkkosivustoille. Turvallisen verkkoasioiden hoitamisen kannalta on tärkeää käyttää vain luotettavia ja turvallisia verkkosivustoja ja palveluita. Voidaankin todeta yhteenvetona turvallisesta asioinnista verkossa, että verkon käyttäminen vaatii aktiivista osallistumista ja huolellisuutta. Noudattamalla hyviä turvallisuuskäytäntöjä ja pysymällä tietoisina verkossa vaanivista riskeistä voidaan varmistaa, että verkkoasiointi pysyy turvallisena ja suojattuna.

5.2 Tutkimuksen tuloksista (Maksuvälinepetosten tilanne)

Maksuvälinepetokset tulevat tilastojen valossa ja digitalisoituvan yhteiskunnan kasvaessa yhä globaalisemmassa toimintaympäristössä – siis kaikessa kanssakäymisessä niin sosiaalisesti kuin kaupallisesti. Tämä tarkoittaa kyseiselle rikoslajille yhä enemmän mahdollisuuksia toteutua, kun mahdollisia tilanteita nousee jatkuvasti. Lainsäädäntö ja muut kontrolloivat toimenpiteet valitettavasti seuraavat kehitystä ja usein vain pystyvät reagoimaan esille nousseisiin haasteisiin. Maksuvälinepetoksien torjunnassa on pystyttävä moniviranomaisesti ja moniasiantuntijoiden osaamisella kehitettävä turvallisempia maksuvälineitä ja kaupankäyntimahdollisuuksia. Kaksiosainen varmenne, digitaalinen lompakko, osaamisen lisääminen verkkoympäristössä etenkin potentiaalisten riskiryhmien osalta sekä pankki- ja luotonantajien korostettu huolellisuusvelvollisuus varallisuuden siirroissa tulevat mielestäni olemaan avainasemassa torjuttaessa maksuvälinepetoksia.

Maksuvälinepetos on osa petosrikollisuuteen liittyvää rikollisuutta, jonka ominaispiirteitä on löytää turvallisina pidetyistä maksuketjuista heikkouksia. Maksuvälinepetos – vaikka ei tunnusmerkistöltään ole yhtä kattava kuin perinteinen petos – toteutuakseen tarvitsee jossain kohtaa ketjua heikon kohdan. Heikko kohta voi olla, vaikka hyväuskoisuus, luottamus tai alkurikoksella saatu maksuväline. Kyse on kuitenkin rikollisen toiminnan kriminalisoinnista ja sen rikosoikeuden pyrkimyksestä yhteiskunnan oikeustilan normalisoinnista. Kyse on kuitenkin suhteellisen uudesta rikoslajista rikosoikeudessa johtuen maksutapahtumien muutoksesta, käteisestä verkkomaailmassa tapahtuvien virtuaalivaluuttojen bittimaailmaan.

Maksuvälineet ovat kehittyneet hurjasti ja vaihtoehtoja maksamiselle on lukuisia. Maksuvälineet ovat tarkoitettu olemaan turvallisia ja niiden oikea oppinen ja turvallinen käyttö ennalta ehkäisisi maksuvälinepetoksia ja maksuvälineisiin liittyviä vahinkoja. Tässä opinnäytetyössä käsiteltiin maksuvälineitä, jotka sisältävät yksilöivän tunnisteen. Yksilöivät tunnisteet ovat välttämättömiä, kun on kyse maksamisesta, jotta voidaan osoittaa maksuvälineen haltija ja varat, joita voidaan käyttää

maksuvälineen avulla. Nykyisin maksuvälineet ovat äärimmäisen nopeita ja helppokäyttöisiä, mikä lisää vahingon riskiä. Maksuvälineiden käyttö muokkautuu käyttäjien mukaan jatkuvasti ja tulevaisuudessa maksuvälineet tulevat kehittymään entisestään, mutta maksamisen nopeus ja helppous, eivät paljoa nykyisestä voi enää kehittyä, kun maksutapahtuma suoritetaan silmän räpäyksessä.

Maksuvälinepetoksia voi tehdä monella tapaa ja tekotapojen kirjo on laaja. Tekotapoja on niin erilaisia, kun on tekijöitäkin, vaikka tietyt peruselementit maksuvälinepetoksesta aina löytyykin. Tietoverkossa tapahtuvat maksuvälinepetokset ottavat koko ajan enemmän tuulta alleen ja ne tekotavat ja tekniikat, joita nyt on viranomaisten tiedossa, voivat olla joillekin rikoksen tekijöille jo menneen talven lumia.

Yhteenvetona voidaan todeta, että maksuvälinepetosten nopea ja jatkuva kehitys on monimutkainen ilmiö, jonka torjuminen vaatii laajaa yhteistyötä eri viranomaisten välillä, sekä ennen kaikkea erityistä osaamista.

5.3 Kehitysehdotukset

Tärkeä investointi kohde mielestäni on ihmisten valistaminen internetin vaaroista. Tietoa on saatavilla runsaasti niin kirjallisuudessa kuin verkkoartikkeleissakin, erityisesti englanninkielisillä sivustoilla. Tietoa maksuvälinepetoksilta suojautumiseen ja torjuntaan on valtavasti tarjolla ja sitä tulisikin seurailla silloin tällöin, jotta verkossa ei tule surffattua suoraan ansaan. Poliisi.fi sivustolta löytyy ajankohtaista tietoa aiheesta, sekä miten toimia, jos on joutunut maksuvälinepetoksen uhriksi. Mielestäni poliisin tulisi lisätä tiedottamista siitä, miten suojautua näiltä rikoksilta, joka voisi jo osaltaan ennaltaehkäistä räikeimpiä huijausyrityksiä onnistumasta. Erityisesti sosiaalinen media voi toimia tehokkaana tiedotusvälineenä, etenkin nuoremmalle sukupolvelle. Myös vanhemmille, jotka osaavat internetin käytön peruselementit, mutta eivät välttämättä ole täysin tietoisia internetin vaaroista.

Mielestäni jokaisen internettiä käyttävän aikuisen tulisi käyttää virtuaalista erillisverkkoa (VPN) vähintään tehdessään töitä internetissä ja mieluiten, myös vapaa-ajan nettisurffailuissa. VPN käyttö on lisääntynyt ja uskon vahvasti, että se toisi tietynlaisen virtuaalisen muurin tietoverkkoavusteisten maksuvälinepetosten, sekä koko internetrikollisuuden ja kansalaisten välille. Tänä päivänä markkinoilta löytyy paljon laadukkaita tietoturvaohjelmia, jotka ovat hyödyllisiä apuvälineitä internettiä käyttävälle. Tärkeimpänä suojautumiskeinona maksuvälinepetoksilta ja samalla muiltakin internetin vaaroilta, pidän jokaisen omaa tietoisuutta siitä, mitä on tekemässä ja millä alustalla. Erityisesti tämä pätee, kun olet tekemisissä maksuvälineiden kanssa. Kiteytettynä voidaan sanoa, että terveen järjen käytöllä pääsee pitkälle ja törmätessäsi liian hyvään tarjoukseen verkossa, niin se todennäköisesti juuri on liian hyvä ollakseen totta.

Jatkotutkimusta aiheesta voisi tehdä asianomistajan profiloinnin ja tietoisuuden merkityksestä maksuvälinepetoksiin verkossa. Tätä voitaisiin tarkastella, myös siltä kannalta, mihin poliisin kannattaa kohdistaa resursseja verkkorikollisuuden ennalta estävässä toiminnassa. Aihe on ajankohtainen, sillä jatkuva tietoverkko avusteisten maksuvälinepetosten ohjaa, myös poliisin toimintaa.

6 POHDINTA

Tässä osiossa on tarkoituksena arvioida opinnäytetyöprosessia ja sen onnistumista. Opinnäytetyö oli itselleni ensimmäinen ja se toi omat haasteensa etenkin oikeanlaisen opinnäytetyön tekemiselle. Kirjoittaminen, sekä aiheen löytäminen ei tuottanut ongelmia, sillä tiesin jo koulutuksen alkuvaiheessa, että opinnäytetyö tulee liittymään verkkorikollisuuteen. Verkkorikollisuudesta ja sen monimuotoisuudesta, oli tietoa kerääntynyt jo siviilielämän puolelta, joten maksuvälinepetoksiin perehtyvä opinnäytetyö oli itselle mielenkiintoinen tutkimuskohde. Siviilielämän puolelta hankittu tieto lähinnä auttoi hahmottelemaan kokonaisuutta ja kaikki sisältötieto kertyi julkisista lähteistä tutkimuksen aikana. Tämä osaltaan tuo tutkimukselle autenttisuutta ja luotettavuutta, kun tutkimus on tehty tutkimusmenetelmien mukaisesti.

Opinnäytetyön aiheeseen liittyvän kirjallisuuden ja muun materiaalin hankkiminen ei ollut haastavaa, koska työ oli tutkimuksellinen. Vastauksia tutkimuskysymyksiin löytyi pääosin lainvalmisteluaineistoista. Metodina käytin lainopillista tutkimustapaa, sekä kirjallisuuskatsausta, jotka ovat vakiintuneita menetelmiä tällaisissa opinnäytetöissä. Tässä työssä kohtaamani haaste oli se, että uusien lähteiden tutkiminen johti jatkuvasti uusiin löytöihin ja ideoihin. Tämä toi mukanaan riskin siitä, että työn laajuus kasvaisi liian suureksi, eikä kaikkia löydettyjä lähteitä eikä ideoita ollut mahdollista käsitellä tutkimuksen puitteissa.

Jo lainvalmisteluaineistossa selvitettiin suoraan muutosten taustalla olevia syitä, pystyi muista lähteistä, kuten kirjallisuudesta, lakiesitysten lausunnoista ja julkisista mielipiteistä, tekemään omia johtopäätöksiä siitä, miksi näitä lausuntoja annettiin ja mitä taustalla tapahtui. Olisi ollut hyödyllistä ottaa mukaan myös kansainvälistä aineistoa laajuuden lisäämiseksi, mutta opinnäytetyön rajausten vuoksi tämä olisi voinut olla haastavaa. Tärkeänä pidin kuitenkin tutkimuskysymysten ja aiheen rajauksien pitämistä mielessä. Kokonaisuutena opinnäytetyöprosessi oli mielestäni onnistunut, ja sain vastauksia tutkimuskysymyksiini.

LÄHTEET

Aarnio, A. 1989: Laintulkinnan teoria. Yleisen oikeustieteen oppikirja. Porvoo, Helsinki, Juva, WSOY.

Aurejärvi, E., & Hemmo, M. 2004: Luotto-oikeuden perusteet. Helsinki. Talentum Media.

Apple. 2024: Tee ostoksia Apple Paylla. Verkkosivu. Luettavissa: https://support.apple.com/fi-fi/HT201239. Luettu 18.5.2024.

Bittimaatti. 2023: Suomen Bitcoin-automaattiverkosto. Verkkosivu. Luettavissa: https://bittimaatti.fi/ . Luettu 19.5.2024.

Enisa. 2019: ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends. Verkkosivu. Luettavissa: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 . Luettu 12.5.2024.

Enisa. 2023: ENISA Threat Landscape Report 2023. Verkkosivu. Luettavissa: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 . Luettu 13.5.2024.

Finanssiala. 2023: Maksutavat 2022 – tekstiraportti. Julkaisut ja tutkimukset 2023. Luettavissa: https://www.finanssiala.fi/wp-content/uploads/2023/02/maksutavat-2022.pdf . Luettu 12.5.2024.

Finanssivalvonta. 2024: Maksamiseen liittyvät petokset ja huijaukset kasvava ilmiö – Finanssivalvonnan selvityksen mukaan pankkiasioinnin turvallisuutta mahdollisuus parantaa. Verkkosivu. Luettavissa: https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/lehdistotiedotteet/2024/maksamiseen-liittyvat-petokset-ja-huijaukset-kasvava-ilmio--finanssivalvonnan-selvityksen-mukaan-pankkiasioinnin-turvallisuutta-mahdollisuus-parantaa/ . Luettu 10.5.2024.

Hallamaa, T. 2020: Oletko huomannut? Käteinen on lähes kadonnut muutamassa vuodessa, mutta digitaalisuus vaikeuttaa rahan hahmottamista. Verkkosivu. Luettavissa: https://yle.fi/uutiset/3-11166192 . Luettu 11.5.2024

HE 38/1997. Hallituksen esitys Eduskunnalle laiksi rikoslain 37 luvun muuttamisesta.

HE 52/2021 vp. Hallituksen esitys eduskunnalle laiksi rikoslain 37 luvun muuttamisesta.

Johansson, K. & Axelin, A. & Stolt, M. & Ääri, R. 2007: Systemaattinen kirjallisuuskatsaus ja sen tekeminen. Turku. Turun yliopisto.

KKO 1999:110.

KKO 2019:44.

Kangasniemi, T. 2012: Identiteettivarkaudet – haasteita rikostukinnalle ja -oikeudelle, paljon vaivaa ja harmia uhrille, perus- ja ihmisoikeudet rikosprosessissa. Teoksessa Ervo & Lahti & Siro 2012. Helsinki, Helsingin Hovioikeus. Hakapaino Oy, 217-238.

Kolttola, I. & Beuker, A. 2023: Rikollisuustilanne 2022: rikollisuuskehitys tilastojen ja tutkimusten valossa. Helsingin yliopisto, Valtiotieteellinen tiedekunta, Kriminologian ja oikeuspolitiikan instituutti. Katsauksia 55/2023.

Kunelius, J. 2017: Mitä skimmaus on? Poliisiammattikorkeakoulu. AMK-opinnäytetyö.

Lehtonen, A. 2016: Nettipetosten kasvu 2010-luvulla. Poliisiammattikorkeakoulu. AMK-opinnäytetyö.

Mobile transaction. 2020: Maksupäätteiden historia – menneisyydestä nykypäivään. Verkkosivu. Luettavissa: https://fi.mobiletransaction.org/maksupaatteiden-historia/ . Luettu 17.5.2024.

Pagliery, J. 2014: Bitcoin and the future of money. Yhdysvallat, Triumph books.

Piira, M. 2022: Verkkoavusteisten petosten sääntely ja torjunta talousrikosoikeudellisesta näkökulmasta. Lapin yliopisto. Oikeustieteiden tiedekunta. Maisteritutkielma.

Rosenberg, E. 2021: How Does Bitcoin Work? Verkkosivu. Luettavissa: https://www.thebalance.com/how-does-a-bitcoin-transaction-work-391213 . Luettu 18.5.2024.

Suomen Pankki. 2018: Bitcoin ja muut kryptovarat. Verkkosivu. Luettavissa: https://www.suomenpankki.fi/fi/media-ja-julkaisut/kalenteri/tapahtumat/suomen-pankki/2018/bitcoin-ja-muut-kryptovarat/ . Luettu 20.4.2024.

Tapani, J. 2013: Keskeiset rikokset. Teoksessa Frände & Matikkala & Tapani & Tolvanen & Viljanen & Wahlberg. Helsinki, Edita.

Tekniikan Maailma. 2017: Pankkikortilla tapahtuvasta lähimaksusta löytyi tietoturvauhka – näin voro voi käyttää sitä hyväksi. Verkkosivu. Luettavissa: https://tekniikanmaailma.fi/tm-testasi-pankkikortilla-tapahtuvasta-lahimaksusta-loytyi-tietoturvauhka-nain-voro-voi-kayttaa-sita-hyvaksi/ . Luettu 14.5.2024.

Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar. 2022: Cybercrime and Digital Forensics, An Introduction. New York, Routledge.

Tilastokeskus. 2024: StatFin. Verkkosivu. Luettavissa: https://pxdata.stat.fi/PxWeb/pxweb/fi/StatFin/ . Luettu 15.4.2024.

Vakuutus- ja rahoitusneuvonta, a. 2024: FINE- 025772, Ratkaisusuositus - FINE-026772 - FINE - Vakuutus- ja rahoitusneuvonta. Luettu 18.5.2024.

Vakuutus- ja rahoitusneuvonta, b. 2024: FINE 000793 (2017), Ratkaisusuositus - FINE-000793 - FINE - Vakuutus- ja rahoitusneuvonta. Luettu 18.5.2024.

Yle. 2010: Elävä arkisto: Rahat kortilla. Verkkosivu. Luettavissa: https://yle.fi/aihe/artikkeli/2010/06/10/rahat-kortilla . Luettu 16.5.2024.

Yle. 2016: Asiantuntija: Lähimaksukortilta voi imuroida rahaa salaa, mutta varas jää kiinni. Verkkosivu. Luettavissa: https://yle.fi/a/3-8682936 . Luettu 13.5.2024.

IOCTA. 2023: Internet Organised Crime Assessment. Verkkosivu. Luettavissa: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023 . Luettu 16.5.2024.